Xtralis VSM4

Product Guide

November 2010
Document: 11885_08
Part Number: 20536

xtralis
The sooner you know™

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a licence or any other right to use the name and/or trademark and/or label.

This document is subject to copyright owned by Xtralis AG ("Xtralis"). You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify or publish any contents of this document without the express prior written consent of Xtralis.

Disclaimer

The contents of this document is provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Xtralis. All proper health and safety precautions must be taken during the installation, commissioning and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Xtralis is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Xtralis accredited training course can install, test and maintain the system.

Liability

You agree to install, configure and use the products strictly in accordance with the User Manual and product documents available from Xtralis.

Xtralis is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation or advice given by or on behalf of Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis in relation to the products is limited to:

i. in the case of services, the cost of having the services supplied again; or
ii. in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Xtralis harmless for any claim, cost, demand or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

Document Conventions

The following typographic conventions are used in this document:

Convention	Description
Bold	**Used to denote:** emphasis Used for names of menus, menu options, toolbar buttons
Italics	**Used to denote:** references to other parts of this document or other documents. Used for the result of an action.

The following icons are used in this document:

Convention	Description
	Caution: This icon is used to indicate that there is a danger to equipment. The danger could be loss of data, physical damage, or permanent corruption of configuration details.
	Warning: This icon is used to indicate that there is a danger of electric shock. This may lead to death or permanent injury.
	Warning: This icon is used to indicate that there is a danger of inhaling dangerous substances. This may lead to death or permanent injury.

Contact Us

The Americas	+1 781 740 2223
Asia	+852 2916 8894
Australia and New Zealand	+61 3 9936 7000
Continental Europe	+32 56 24 19 51
UK and the Middle East	+44 1442 242 330
www.xtralis.com	

Table of Contents

1 Introduction **3**
- 1.1 VSM4 Software 3
- 1.2 Product Guide 4
- 1.3 Communications 4
- 1.4 Help System 5

2 Installation **7**
- 2.1 Software Installation 7
- 2.2 Starting VSM 9
- 2.3 Install Optional Features 18
- 2.4 Logon 20
- 2.5 General Options 22
- 2.6 Exit Application 22

3 Designing a Monitored System **23**
- 3.1 The Monitored Structure 23
- 3.2 Remote Notification 32
- 3.3 Verification 39
- 3.4 Events 40

4 Monitoring **45**
- 4.1 Observation 45
- 4.2 Monitored Conditions 51
- 4.3 Acknowledging an Incident 52
- 4.4 Event Management Options 53
- 4.5 Device Status 54
- 4.6 Connection Status 60

5 Investigation **61**
- 5.1 Investigation Tools 61

6 Administration **69**
- 6.1 System Access 69
- 6.2 Resource Management 73
- 6.3 Software Upgrades 76

7 Views **77**
- 7.1 Common Behaviour 77
- 7.2 Integrated Active Event List 78
- 7.3 Status Bar 82
- 7.4 Floor Plan 83
- 7.5 HTML Browser 93
- 7.6 Device Status View 95
- 7.7 Monitor Browser 97
- 7.8 Device View 102
- 7.9 Trend Graph 103
- 7.10 Event Log View 108

8 Workspace Configuration **111**
- 8.1 Display Structure 111
- 8.2 View Management 111
- 8.3 Multiple Displays 112
- 8.4 Automatic Frame Behaviour 113

A Prerequisites **115**

A.1 Monitoring Computer 115
A.2 Network Capacity 116

B Checklists 117

B.1 Planning Checklist 117
B.2 IT Checklist 118

C Serial to Ethernet Connection 121

C.1 Example Configuration 121
C.2 Serial to Ethernet Device Selection 123
C.3 Network Requirements 123
C.4 Software Installation and Configuration 124

D Define a Connection 129

D.1 VESDAnet Connection via HLI 130
D.2 MODBUS RS-485 Connection via RS232-RS485 Converter 131
D.3 VESDAtalk and VESDAlink Standalone Device Connection 132
D.4 RS-232 MODBUS Standalone Device Connection 134
D.5 TCP/IP MODBUS Standalone Device Connection 136

1 Introduction

Welcome to the VSM4 Product Guide.

This document describes the main features of VSM4 and provides information on how to install and use the software.

For specific information on individual fire protection system hardware components, refer to the Xtralis ICAM and Xtralis VESDA System Design Manuals.

1.1 VSM4 Software

VSM4 is a software-based fire protection system monitoring and control center. It provides a suite of tools for use with Xtralis VESDA and ICAM fire protection systems.

Primary features that comprise each standard VSM4 installation include:

- Advanced fire protection system monitoring and control
- Floor Plan integration, allowing ready visualization of the locations of all incidents
- An integrated browser allows users to link their own response documents to incidents
- Optional email and SMS notification allows remote users to be informed when where the notification trigger events occur. The messages are completely customizable
- Analysis tools include access to event logs and the ability to graph historical and live data for detectors
- Optional audible annunciation of fire and fault conditions (Text-to-Speech)
- Network, System and Device level configuration tools
- Maintenance and troubleshooting tools

VSM4 can be used continuously in monitoring stations where 24 hour observation is necessary or on demand at sites where full-time monitoring is not required.

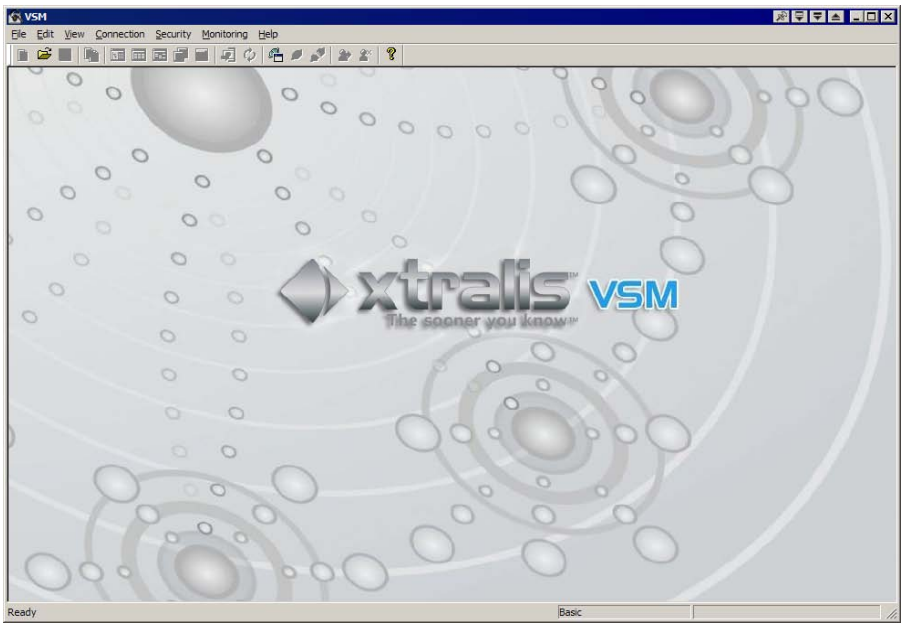


Figure 1-1: VSM4 Main Window

Detailed information on each feature can be found in the appropriate chapters of this Product Guide. See below for a summary of the contents of each chapter. Additional information is available in the help system.

1.2 Product Guide

Chapters contained within this Product Guide contain information describing how to install and then work with the system. The Design and Monitoring functions of the VSM4 application are described first:

- **Chapter 2 - Installation:** This chapter provides information on installing and licensing the software on a monitoring computer.
- **Chapter 3 - Designing a Monitored System:** This chapter explains how to create a system that normal operators can use to monitor a site by integrating multiple networks into a monitored structure and then linking these to active regions on a floor plan. Instructions on setting up email notifications are also covered.
- **Chapter 4 - Monitoring:** This chapter describes how an operator may use the software to monitor a fire protection system. This includes responding to alerts and alarms and then drilling down to detailed device status.
- **Chapter 5 - Investigation:** This chapter describes the tools to review current and past detector performance and state, so that past incidents can be investigated.
- **Chapter 6 - Administration:** This chapter provides information for administrators to be able to maintain a VSM4 installation.
- **Chapter 7 - Views:** This chapter describes the range of views that are provided to allow various aspects of the system to be monitored and controlled.
- **Chapter 8 - Workspace Configuration:** This chapter describes how to customize various display aspects.
- **Appendix A - Prerequisites:** This appendix provides the minimum recommended specifications for the Monitoring Computer.
- **Appendix B - Checklists:** This appendix provides checklists to guide IT administrators in successfully integrating VSM4 with corporate networks.
- **Appendix C - Serial to Ethernet Configuration:** This appendix provides the information required to install and configure Serial to Ethernet devices.
- **Appendix D - Define a Connection:** This appendix details the procedures used for defining connections between VSM4 and devices or networks.

1.3 Communications

VSM4 is able to directly communicate with:

- VESDAnet network(s) using a High Level Interface (HLI) per network
- VLF smoke detectors using the VESDAtalk protocol
- Single or multiple VLC (RO) smoke detectors using the VESDAlink protocol
- Multiple individual VFT and IFT detectors using Modbus over RS232 and IP
- Multiple VFT or IFT detectors on Modbus RS485 Networks
- Multiple individual VESDA ECO and ICAM ECO detectors using Modbus over USB
- Multiple VESDA ECO and ICAM ECO detectors on Modbus RS485 Networks

Remote networking can be achieved for VESDA and ICAM detectors via many technologies, providing they support serial data communications. Connectivity via the use of IP-based LAN and WAN networking is supported via serial port emulation (e.g. MOXA devices). Refer to Appendix C for further information. A TCP/IP interface on an IFT or VFT detector also enables a remote connection to the Monitoring PC through the LAN/WAN.

1.4 Help System

VSM4 contains an extensive context-sensitive help system which provides information on software features and operational procedures.

Using the Help System

- **Invoke the Help System -** Press F1 at any time while using the software, or select **Help > VSM4 Help** from the menu system.
- **Browse -** Use the Table of Contents tab to open topics on subjects of interest. Navigate between help topics by following hyperlinks available in related topic lists or within the help text.
- **Search -** Locate specific information by entering keywords into the field in the search tab and pressing Enter. Alternately, click the List Topics button, then select from the list of topics that contain the keywords. If a search gives no results, try using alternate keywords or varying the wording of a sentence.

An example topic of the VSM4 Help System can be seen below (Figure 1-2).

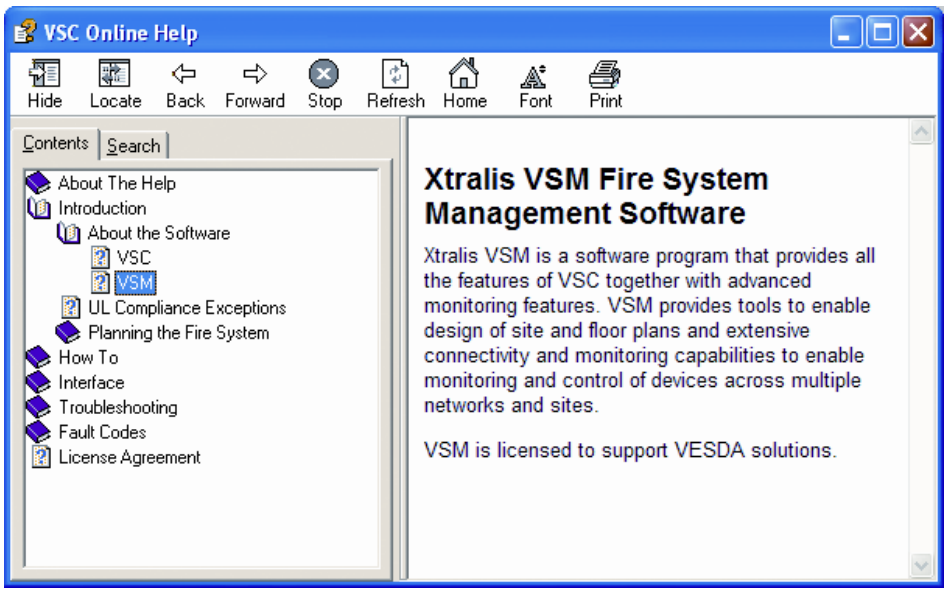


Figure 1-2: VSM4 Help System

This page is intentionally left blank.

2 Installation

This chapter describes how to install VSM4 at your site.

Note: The following instructions are for the installation and configuration of VSM4 software only. Instructions for the installation and operation of fire protection system equipment are available in other documents.Refer to the Xtralis VESDA or Xtralis ICAM System Design Manual for further information.

The table below outlines all steps required to install VSM4.

Step	Description	Ref
1	Prerequisites	Appendix A
2	Install VSM4	2.1.1
3	Launch VSM4	2.2.2
4	License and Activate Software	2.2.4
5	Install Optional Features	2.3

Table 2-1: Installation Overview

2.1 Software Installation

VSM4 has a simple InstallShield Installation Wizard that guides you through the steps required to install the software. After the Installation Procedure has been completed, it is necessary to correctly license, register and activate the installation.

Note: Before installing the software, check that your system satisfies the minimum requirements listed in Appendix A. The checklist (Appendix B) should be filled out and passed to your IT support staff so that they can ensure that your system is correctly supported and will properly integrate into the corporate network. Once the IT staff have completed setting up your network access and completed the information on the checklist, then you are ready to install the software.

2.1.1 Installation Procedure

1. Log into the computer using an account with local administration privileges.
2. Close all software applications.
3. Insert the software installation disk into the DVD drive.
4. Select **VSM4 Software > VSM4 Installation Program** from the menu system to launch the installation program.
5. If autorun is not enabled, locate the installation program (VSMSetup.exe) on the installation disk and run it.
   The InstallShield Wizard should appear (refer to Figure 2-1 below).

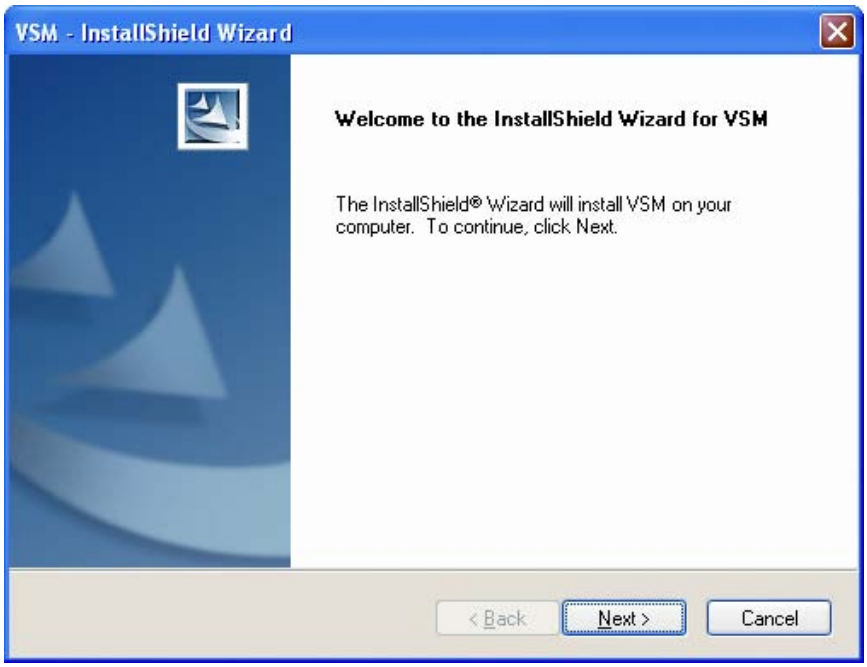

VSM - InstallShield Wizard
Welcome to the InstallShield Wizard for VSM
The InstallShield® Wizard will install VSM on your computer. To continue, click Next.
< Back
Next >
Cancel

Figure 2-1: VSM4 Installshield Wizard

6. Follow the InstallShield Wizard prompts.
7. Launch VSM4 by double-clicking the desktop shortcut or by selecting **Start > Programs > Xtralis > VSM4 > VSM4**.

Installing to Alternate Drive Locations

By default, VSM4 is installed under the "Program Files" directory of the system drive.

It is possible to install the application in an alternative location, however there are potential issues that the installer should be aware of.

VSM4 is protected by a licensing system (refer to section 2.2.4 below), which requires that every installed copy of each product be licensed. The licensing system stores data in multiple locations on the Monitoring Computer. One of these locations is under the application's installation directory.

Once the license has been created for the first time, the licensing system records the drive letter in which the licensing data files were placed. This drive letter must always be available in order for the application to execute or be re-licensed. If the drive letter ceases to be available at any time in the future, it will no longer be possible to execute the software without assistance from Xtralis technical support.

Procedure

To install the application in a location other than "C:\Program Files", select **Start > Run** and start the InstallShield program with the parameter "/setdir" (refer to Figure 2-2 below). This will enable the default drive path to be edited during installation.

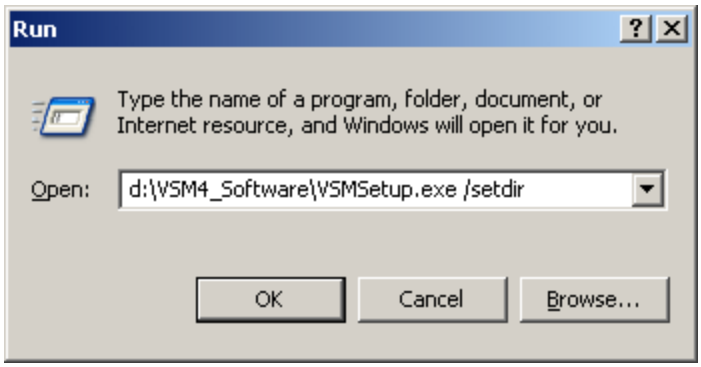


Figure 2-2: Start > Run

2.2 Starting VSM

Before launching VSM4 the Operating system settings should be reviewed as described below.

2.2.1 Computer, Operating System and Software Settings

For best and uninterrupted performance, the following options should be configured where appropriate:

- **Automatic Updates (Operating System, Antivirus) -** If the Monitoring Computer is connected to a network and has internet access, automatic updates should be set to manual, or to run automatically at a time when staff will be available to restart the software in monitoring mode if the Monitoring Computer is automatically rebooted after an update.
- **Screen Savers -** Screen Savers and other power saving options for the display screens should be disabled in the Monitoring Computer BIOS and in the operating system.
- **Additional Software -** If the Monitoring Computer is used in a critical environment, installation of other software applications should be limited. Checking of email and insertion of disks or other memory drives should also be restricted, to reduce the possibility of viral infection, configuration conflicts or file system or registry corruption occurring.

Note: Refer to Appendix A - Prerequisites for further information.

2.2.2 Launch VSM4

The software installer places shortcuts in the Start Menu and on the Windows Desktop.

To run VSM4, follow the steps below:

- Double-click the VSM4 shortcut on the Windows desktop;
  or
- Double-click a Floor Plan shortcut on the Windows desktop;
  or
- Select **Start > Program Files > Xtralis > VSM4 > VSM4** from the Windows menu system.

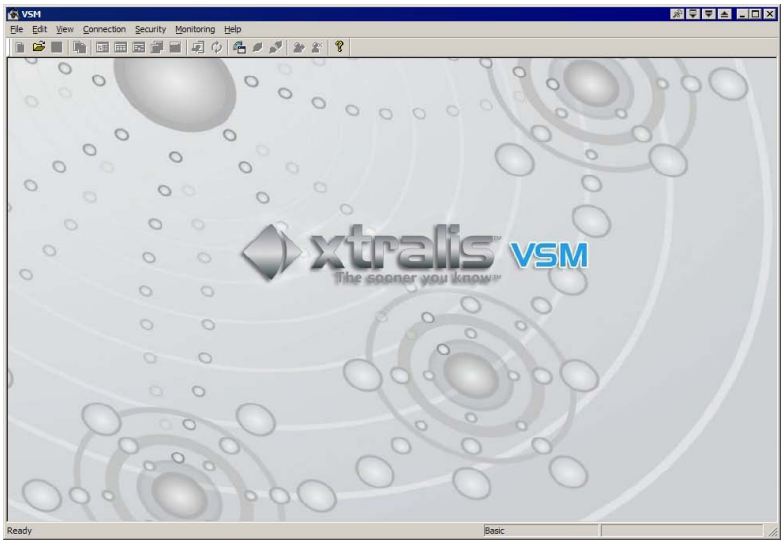


Figure 2-3: VSM4 Software

Set the Default Passwords

The first time VSM4 is launched after installation, you will be prompted to enter a new password for the designer user. Enter the password in both the new password and confirmation fields and select **OK**. The password must contain between 6 and 12 alphanumeric characters.

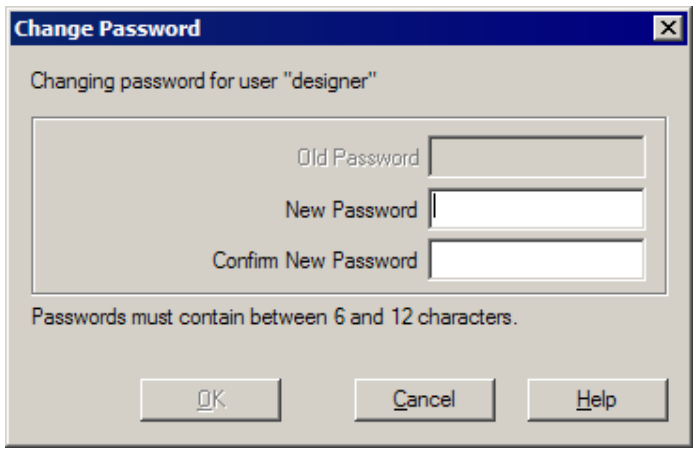


Figure 2-4: Set Designer User Password

Note: It is recommended that the password be recorded in a secure location, as resetting the designer user password requires assistance from your authorized Xtralis representative.

Both the default Administrator and User accounts require that their passwords be defined. To do this, log on as Administrator and enter twelve zeros. You will be prompted to enter your own password.

Repeat this for the default user account.

2.2.3 Monitoring Mode

VSM4 supports two monitoring modes, Primary and Secondary, which define how the PC will manage device event logs.

- The Primary instance of VSM4 is responsible for retrieving events from each monitored device and writing them to the appropriate database.
- Secondary instances of VSM4 can read events from the database or directly from each monitored device but cannot write events to the database.
- In all other aspects, the Primary and Secondary instances of VSM4 operate identically.

Only one PC in a system should run as the Primary system; all others should run as secondary systems. By default, VSM4 starts in Secondary mode.

Primary Monitoring Mode Configuration

To start VSM4 in Primary monitoring mode, follow the steps below:

1. Right-click on the existing shortcut to VSM4 on your desktop, as created by the installation program, and select Properties.
2. In the General tab, rename the shortcut to VSM4 - Primary.
3. Select the Shortcut tab. Refer to Figure 2-5 below.
4. In the target box, add “-primary” to the end of the line. Include a space before adding "-primary" to the target field. Select **OK**.

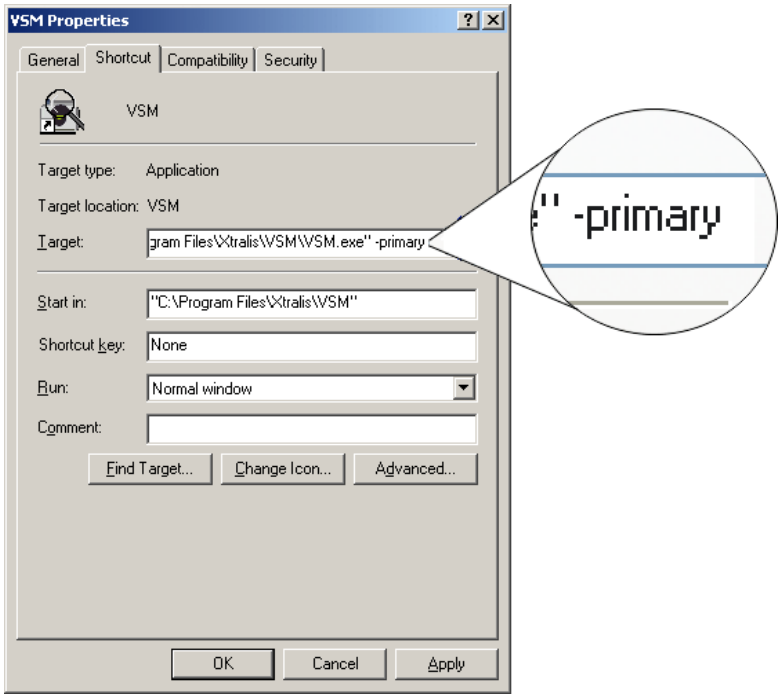


Figure 2-5: VSM4 Shortcut Properties

5. Double-click the shortcut to launch VSM4 in Primary mode.
   VSM4 will indicate that it is running in Primary mode in the title bar of a Monitor Browser view (refer to Figure 2-6 below).

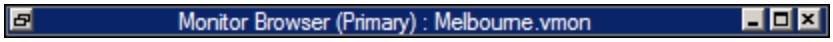


Figure 2-6: VSM4 running in Primary mode

Note: When running in primary mode this is the only way to launch VSM4. Launching VSM4 by double-clicking on a .vmon or .vfp file or via the Start menu will default to Secondary mode.

2.2.4 Licensing and Activation

Once the installation procedure has been completed and the application is launched for the first time, it is necessary to license and activate VSM4.

VSM4 has three types of license, each with varying levels of functionality:

- **Full License -** This provides all purchased features and monitoring capacity, with no expiry time.
- **Demonstration License -** This provides a time period with which to evaluate or demonstrate a system.
- **Evaluation License -** This provides a shorter time period with which to evaluate a system. All VSM4 features can be accessed immediately and used for a 30 day period. Once the time limit has expired, it is necessary to request a Demonstration or Full license in order to continue operating the software.

Refer to the table below for a summary of the differences between each license type:

Function / License	Full	Demo	Evaluation
Time limit	No limit	90 days	30 days
Default features	Design, Configuration, Monitoring	Design, Configuration, Monitoring	Design, Configuration, Monitoring
Monitoring capacity	Token limit set by site license number	660 tokens	660 tokens
Optional features	Text-to-Speech, Remote Notification	Text-to-Speech, Remote Notification	n/a
License request necessary to activate	Yes	Yes	No

Table 2-2: Summary of the differences between the types of licenses

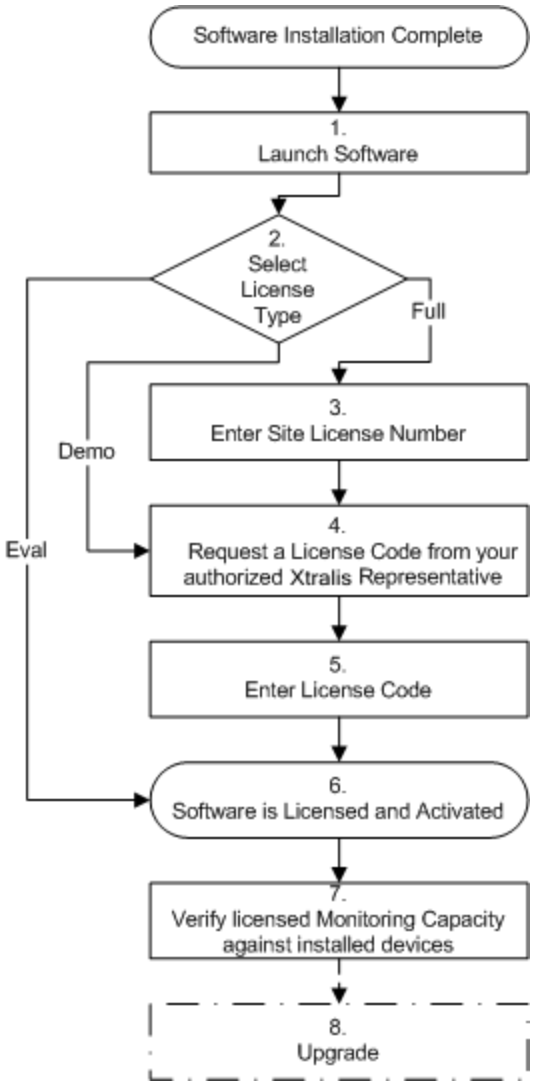


Figure 2-7: Licensing and Activation Overview

Select License Type

- **Full License -** If a full license has been purchased, select Full License by clicking on the radio button. Enter the Site License number (it is usually printed on the DVD case), and click **OK**.
- **Evaluation or Demonstration License -** Select as needed and click **OK**.

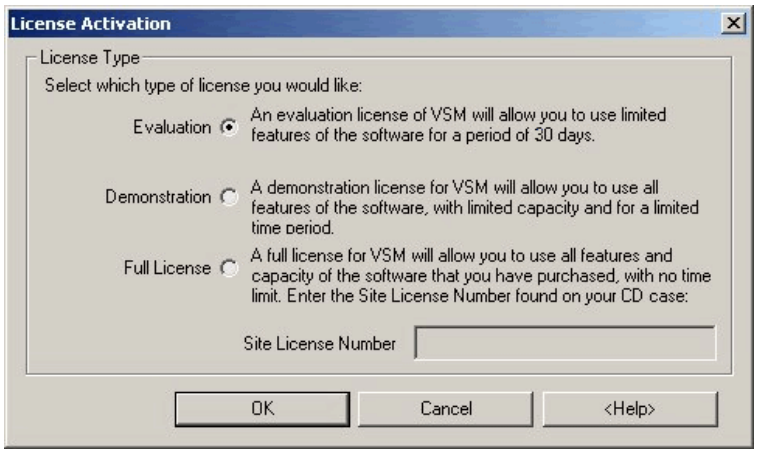

License Activation
License Type
Select which type of license you would like:
Evaluation
An evaluation license of VSM will allow you to use limited features of the software for a period of 30 days.
Demonstration
A demonstration license for VSM will allow you to use all features of the software, with limited capacity and for a limited time period.
Full License
A full license for VSM will allow you to use all features and capacity of the software that you have purchased, with no time limit. Enter the Site License Number found on your CD case:
Site License Number
OK
Cancel
<Help>

Figure 2-8: License type selection

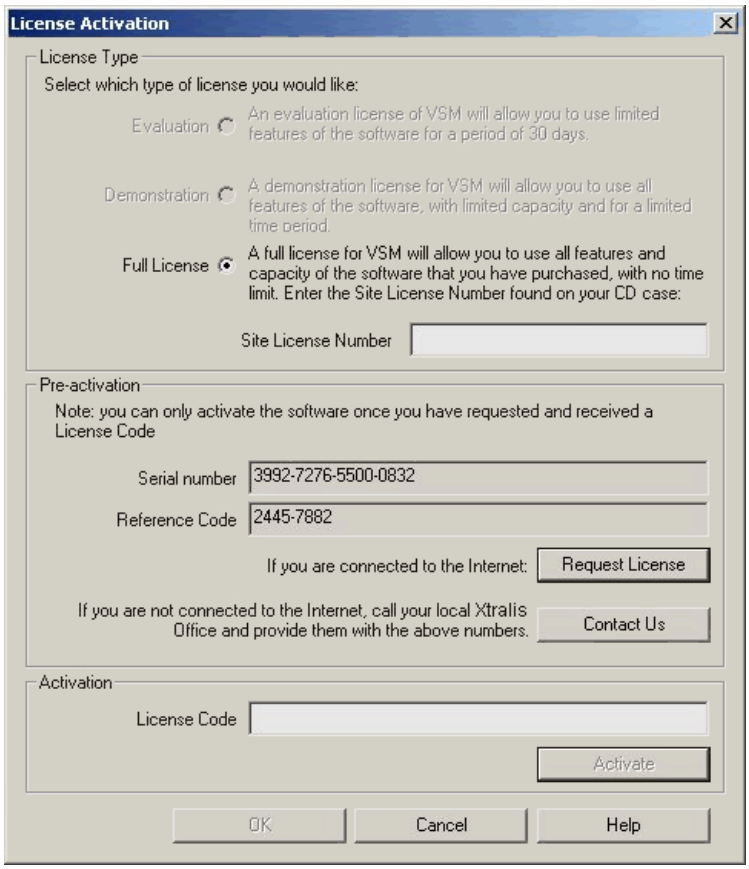

License Activation
License Type
Select which type of license you would like:
Evaluation
An evaluation license of VSM will allow you to use limited features of the software for a period of 30 days.
Demonstration
A demonstration license for VSM will allow you to use all features of the software, with limited capacity and for a limited time period.
Full License
A full license for VSM will allow you to use all features and capacity of the software that you have purchased, with no time limit. Enter the Site License Number found on your CD case:
Site License Number
Pre-activation
Note: you can only activate the software once you have requested and received a License Code
Serial number
3992-7276-5500-0832
Reference Code
2445-7882
If you are connected to the Internet:
Request License
If you are not connected to the Internet, call your local Xtralis Office and provide them with the above numbers.
Contact Us
Activation
License Code
Activate
OK
Cancel
Help

Figure 2-9: Full License Activation

Entering the Site License number or selecting a Demonstration license automatically completes the Serial Number and Reference Code fields. These numbers are required when requesting a License. See below.

Request License

- **Full License or Demonstration License**
  - Where Internet connection is available, select Request License.
    The default web browser will be launched and the Xtralis license code generator form will be displayed. See below (Figure 2-10).
  - Complete the required fields (marked with an asterisk) and select Send.
    An email containing your new License Code will automatically be sent to your nominated email address. If it does not arrive, check if it has been sent into a spam mail area instead of the mail client inbox.
  - Where Internet connection is not available, select **Contact Us**. Phone your authorized Xtralis Representative and provide the Site License Number, Serial Number and Reference Code. A License code will be provided to enter into the License field.
- **Evaluation License: Not applicable**

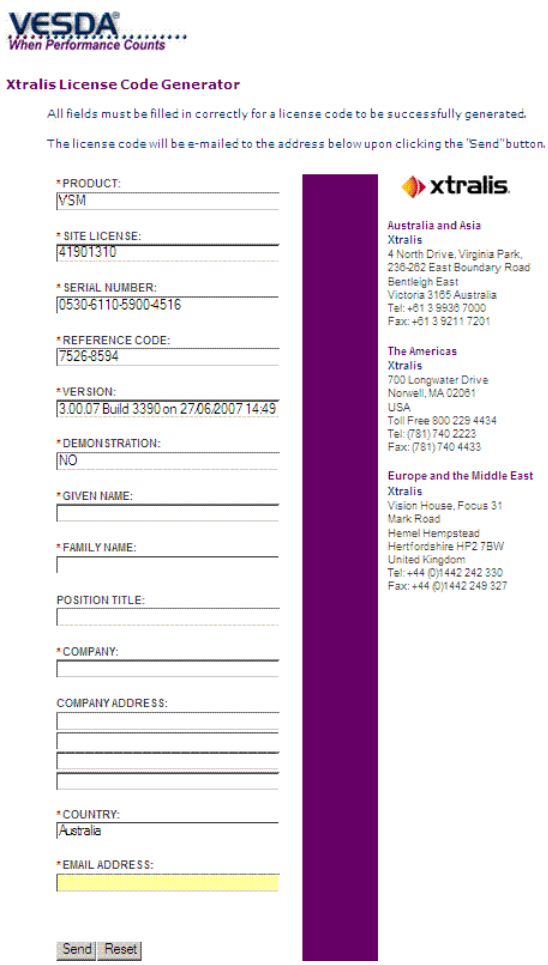


Figure 2-10: Online Activation Request

Enter License Code

- **Full License or Demonstration License**
  - Enter the License code from the email into the License field.
  - For phone activation, enter the License Code provided by your authorized Xtralis representative into the License field.
  - Select **OK** once the software has been successfully licensed (Figure 2-11).
- **Evaluation License: Not applicable.**

Figure 2-11: Licensing and Activation Successful

Note: Software licensing can be upgraded after the initial installation to include additional monitoring tokens or optional features.

2.2.5 Check the Installed Features and Monitoring Capacity

To verify the set of licensed features and monitoring capacity, select **Help > About VSM4** (refer to Figure 2-12).

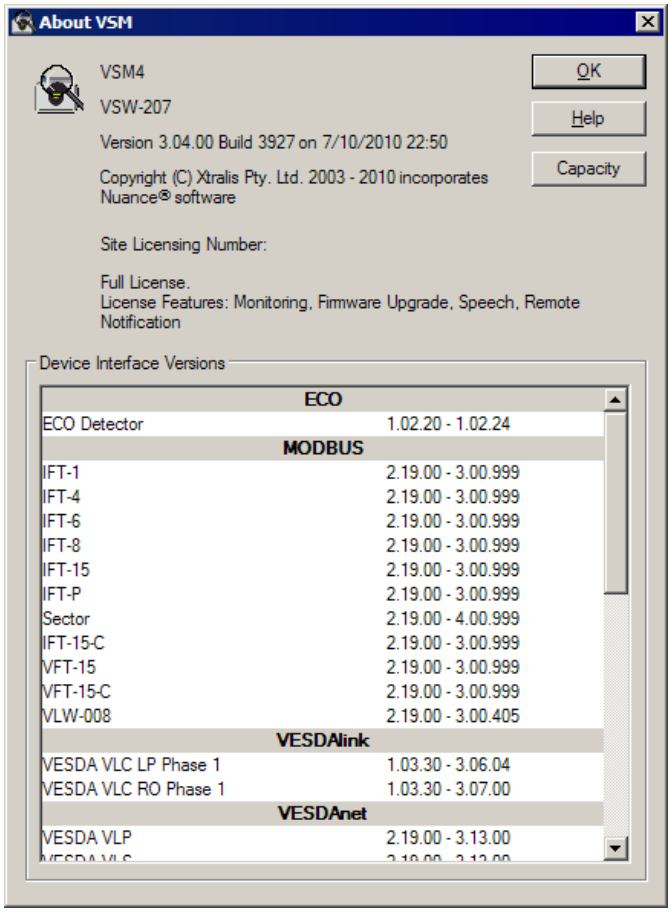


Figure 2-12: About VSM4

Features

The license type and enabled features are displayed in the About VSM4 dialog box.

Available features that should be listed for Full Licenses include the following:

- Monitoring
- Firmware Upgrade
- HTML Viewing
- Remote Notification
- Speech (where the Text-to-Speech optional feature has been enabled)

Figure 2-12 above shows all installed features listed under the license type (in this example, Full License).

Monitoring Capacity

Monitoring capacity is measured by the number of available Connection Tokens. Tokens are used to enable the following:

- **Network Connections -** Each VESDAnet or MODBUS RS-485 requires connection tokens.
- **Detector Connections -** The number of tokens required by monitored detectors are proportional to the sophistication of the detector.

The number of tokens provided with a Full License will have been determined during the purchase and commissioning process. The evaluation and demonstration licenses are both limited to 660 tokens. The activation process is outlined above in Figure 2-7.

For reference, the calculation of the required number of Tokens for each Network Connection or Detector Connection type is as follows:

Networks

- 80 tokens per VESDAnet connection via HLI (High Level Interface) device.
- 80 tokens per MODBUS RS-485 connection via RS485-RS232 converter.

Detectors

- 20 tokens per VLP, VLS, VLC or VLF in a network.
- 20 tokens per IFT-P, IFT-1, IFT-4, IFT-6, IFT-15, VFT-15, VESDA ECO or ICAM ECO connected via the RS485-RS232 converter on a MODBUS RS-485 connection.
- 20 tokens per IFT-P, IFT-1, IFT-4, IFT-6, IFT-15 or VFT-15 connected directly on a MODBUS TCP/IP connection.
- 20 tokens per VESDA ECO or ICAM ECO connected directly via USB.
- 60 tokens per VLF or VLC (RO) connected directly to the monitoring computer via Serial Port.
- 60 tokens per IFT-P, IFT-1, IFT-4, IFT-6, IFT-15 or VFT-15 connected directly to the monitoring computer on a MODBUS RS-232 connection.

For example, a system that consists of a VESDAnet and three VLP detectors on VESDAnet will require 140 tokens: 20 for each of the VLP detectors (the detectors being monitored), and 80 for the VESDAnet (the network being monitored).

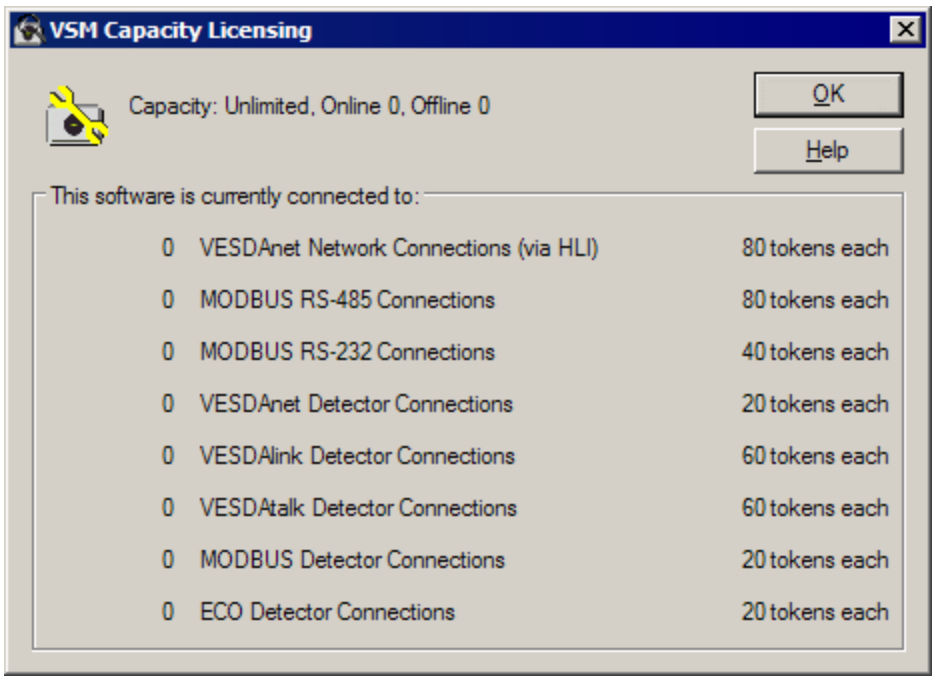

VSM Capacity Licensing
Capacity: Unlimited, Online 0, Offline 0
OK
Help
This software is currently connected to:
0 VESDAnet Network Connections (via HLI) 80 tokens each
0 MODBUS RS-485 Connections 80 tokens each
0 MODBUS RS-232 Connections 40 tokens each
0 VESDAnet Detector Connections 20 tokens each
0 VESDAlink Detector Connections 60 tokens each
0 VESDAtalk Detector Connections 60 tokens each
0 MODBUS Detector Connections 20 tokens each
0 ECO Detector Connections 20 tokens each

Figure 2-13: Monitoring Capacity

If the total token value of all connected devices exceeds the available capacity, network connections will be dropped until the monitored set of devices is equal to or less than the licensed capacity. For increased capacity, contact your authorized Xtralis representative to purchase additional tokens.

2.3 Install Optional Features

Optional features provide additional functionality to the default software installation.

Some optional features are enabled by the software licensing configuration, while others require additional installation procedures to be performed.

2.3.1 Text-to-Speech Voices

Text-to-Speech provides spoken notification of events as they are reported by monitoring devices, in addition to the standard visual and simple audio indications.

Text-to-Speech is based on Nuance's RealSpeak™. Voices are available in multiple languages and dialects, based on either a male or female voice (e.g. 'UK English Emily'). Each voice must be purchased and licensed from Xtralis, then separately installed.

Ordering

If you do not have the Text-to-Speech option and you wish to install it, contact your authorized Xtralis representative for details and purchasing information.

Installation Procedure

1. Log into the computer using an account with local administration privileges.
2. Ensure that Text-to-Speech is appropriately licensed (In the VSM4 application, select **Help > About VSM4** and look for Speech in the enabled features). If Speech is not listed under the licensed features, consult with your authorized Xtralis representative regarding licensing options.
3. Close all software applications.
4. Insert the software installation disk into the DVD drive.
5. Select **VSM4 Software > Text-to-Speech Installation Programs** from the menu system to launch the installation program, and select the appropriate Text-to-Speech installation program.
6. If autorun is not enabled, locate the appropriate Text-to-Speech installation program in the Text-to-Speech folder on the installation disk and run it.
7. Follow the InstallShield Wizard prompts.

RealSpeak UK English Emily - InstallShield Wizard
Welcome to the InstallShield Wizard for RealSpeak UK English Emily
The InstallShield(R) Wizard will install RealSpeak UK English Emily on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

Figure 2-14: Text-to-Speech Installshield Wizard

8. VSM4 will automatically use the newly installed voice. Ensure that the sound speakers are connected correctly to the computer and that the volume controls are set appropriately both on the speakers and in the Operating System volume control. Consult your computer, speaker or operating system documentation for further information.

Troubleshooting

- Confirm that the feature is licensed. Select **Help > About VSM4** and confirm that Speech is listed under the licensed features.
- If there is no sound, verify that the audio system is working on your Monitoring Computer. Check that the speakers are connected to the correct audio input and work by playing windows sample sounds in the Windows Control Panel. Check that the speakers are switched on and that the volume knob is not set to zero. Check that the Wave software volume control (**Start > Program Files > Accessories > Entertainment > Volume Control**) is not set to zero or muted.
- Generate an event on the system. Confirm that the event appears on the Active Event List and that it is sounded by VSM4.

2.4 Logon

Access to VSM4 is controlled and requires users to logon before they are able to use VSM4 to control the monitored detectors. Operators should usually logon with User or Administrator access; Designer access should only be used to setup the monitoring system.

2.4.1 Default Users

Three users are pre-defined for VSM4; Designer, Administrator and User. The first time that the user logs on as Administrator or User they will be prompted to change their password from the default (twelve zeros).

The Designer account name is translated as shown in Table 2-3. The default Administrator and User names are not translated since the Designer should setup custom users and administrators for the site.

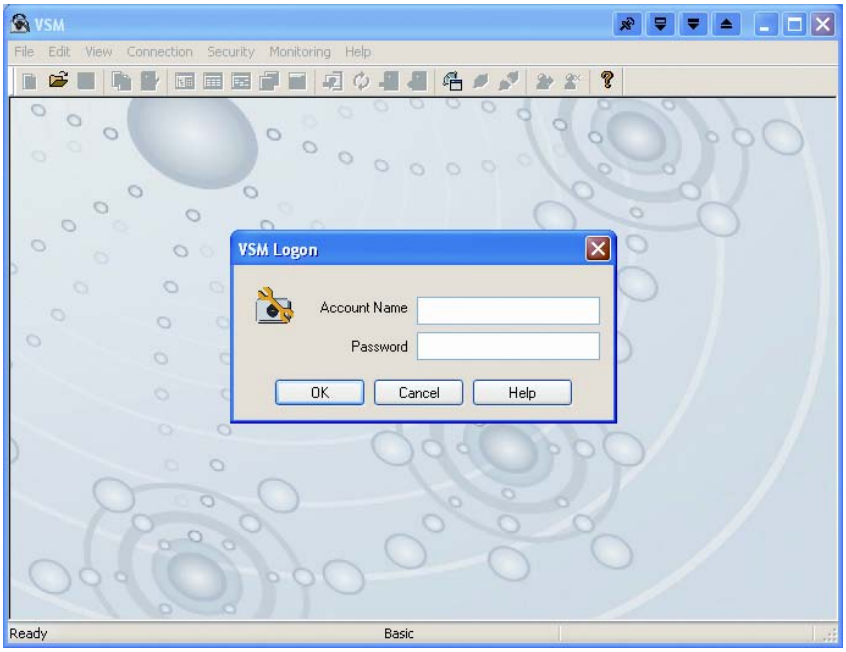


Figure 2-15: VSM4 Logon

Designer User Login for non-English installations

If you are the designer user and VSM4 is operating with a non-English language setting, the login name for the designer user has been translated.

Language	Designer User Login Name
English	Designer
French	Concepteur
German	Designer
Italian	Designer
Polish	Projektant
Russian	Дизайнер
Simplified Chinese	设计者
Spanish	Diseñador
Traditional Chinese	設計者

Table 2-3: Designer User Names

Current Logon Status

The Status Bar, located at the bottom of the VSM4 application window, shows the name of the logged in user and their permission level.

VSM4 starts with the application running at the "Basic" permission level, and no user logged in (refer to Figure 2-16). When a user logs into VSM4, the Status Bar will indicate the user account and the associated access level (refer to Figure 2-17 and Figure 2-18).

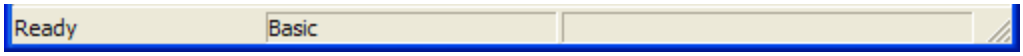


Figure 2-16: Status Bar - Basic (not logged on)

Figure 2-17: Status Bar - Administrator (user "adm" logged on)

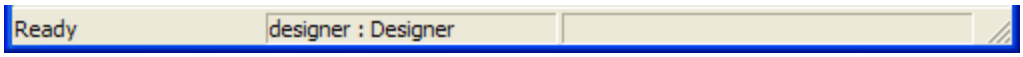


Figure 2-18: Status Bar - Designer (user "designer" logged on)

Change Password

To change your password, follow the steps below:

1. While logged in to VSM4, select **Security > Change Password** from the menu system.
2. Enter the old password, new password and new password confirmation into the appropriate fields.

Passwords need to be between 6 and 12 characters to be valid. They can include numbers, letters and symbols.

2.5 General Options

The General tab of the Options dialog (Figure 2-19) is used to set the language, measurement units, and approvals compliance with the regulatory requirements.

Edit General Options

1. Select **View > Options**.
2. Edit Regional Settings and Approvals as appropriate.
3. Restart VSM4 if either of the language or approvals compliance settings have been changed.

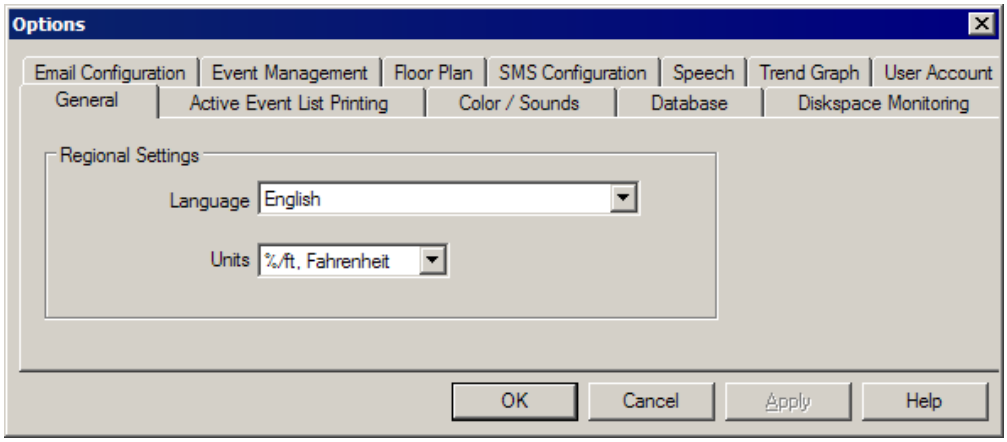


Figure 2-19: View > Options > General

Regional Settings

- **Language -** Select the preferred language for the user interface from the drop down menu.
- **Units -** Select the preferred units (imperial or metric) from the drop down menu. Changes to units are immediately invoked and do not require VSM4 to be restarted.

2.6 Exit Application

VSM4 is a monitoring application and so once it is monitoring a site, it can only be closed by a user logged on with Administrator access.

3 Designing a Monitored System

VSM4 allows a designer to indicate the fire zones that are being monitored by defining the networked devices that are to be monitored and mapping them to Floor Plan regions.

Once these core structures have been defined then the designer can set up email (and SMS) notification for remote personnel. HTML documents can be linked to floor plans to detail the responses that are appropriate to the various contexts being monitored.

This customization of VSM4 to monitor a particular site (or group of sites) is a specialized operation that requires a more in-depth understanding of the software, therefore many of the configuration options are only available when the user is logged on as the Designer. This is also the reason that there is only one Designer user for each VSM4 system.

Once the monitoring system has been built, the Verification Tool allows the user to check the integrity of the structures in order to minimize the testing that the Designer needs to do before the handover to the site operators.

Each of these key steps is described in detail below.

3.1 The Monitored Structure

A Monitoring Site is a logical aggregation of monitored networks. In this structure, the designer creates a logical hierarchy down to a point where connection to a VESDAnet, MODBUS RS-485 network, or standalone Xtralis VESDA or ICAM detector is made.

There is no limit to the depth or breadth of this logical hierarchy, therefore it may be based on business responsibility, geographical location or any other criteria that is relevant to the user.

A major use of the Monitored Structure is as a reference when building up Floor Plans, as described below. Indeed, it is usually the Floor Plans that are viewed by the operators rather than the full Monitored Structure, because they are usually more interested in where an incident is occurring than what network it is on.

3.1.1 Building a Monitored Structure

Building the monitored structure requires the user to be logged in as the designer, and involves starting with a Monitoring Site (select **File > New > Monitoring Site**). A blank Monitoring Site view is displayed which is divided into two vertical panes: the navigation tree on the left and the detailed work area on the right.

Logical Nodes can then be inserted using the **Insert** context menu (refer to Figure 3-1 below).

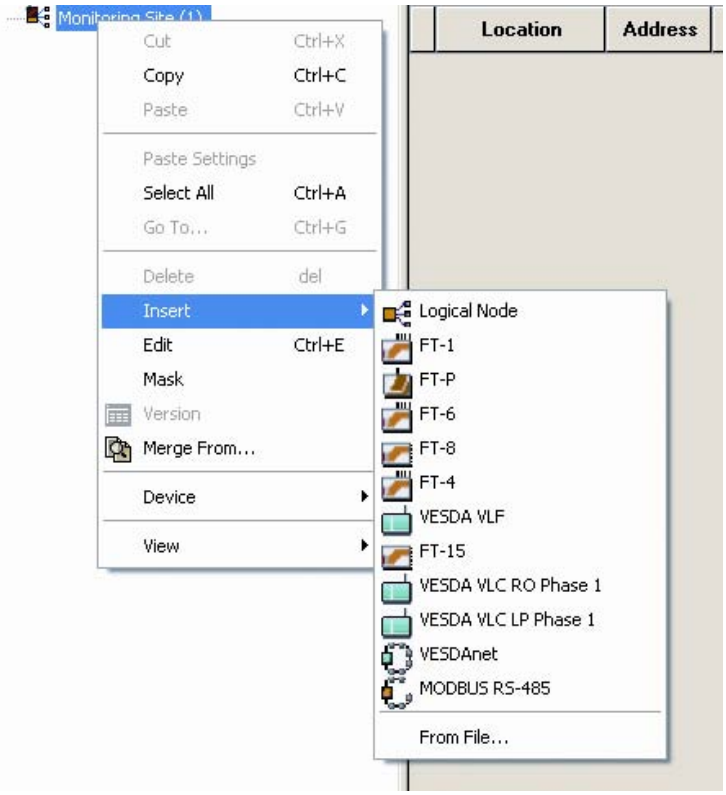


Figure 3-1: Insert Context Menu

As each node is inserted it should be edited to give it a meaningful name.

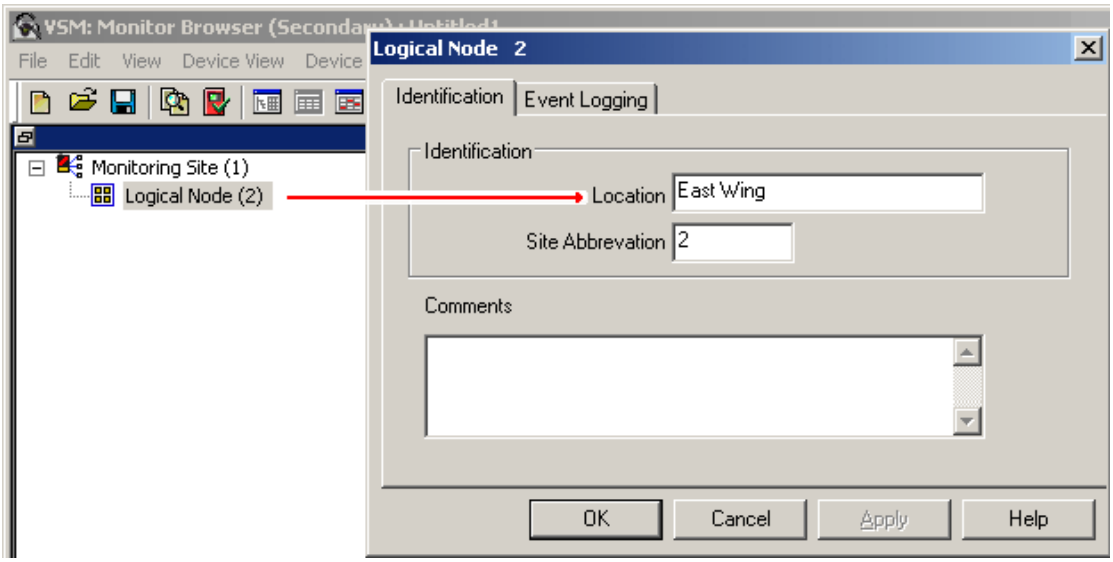


Figure 3-2: Rename Logical Node

At some stage the Designer attaches a network to the logical structure by inserting a VESDAnet or MODBUS RS-485 (refer to Figure 3-3).

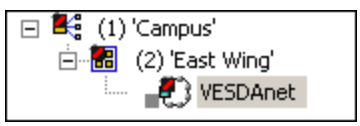


Figure 3-3: VESDAnet Insertion

Detectors and other devices that are physically incorporated within the network are then added to the network. They should be dragged in the grid to the address of the real detector or device.

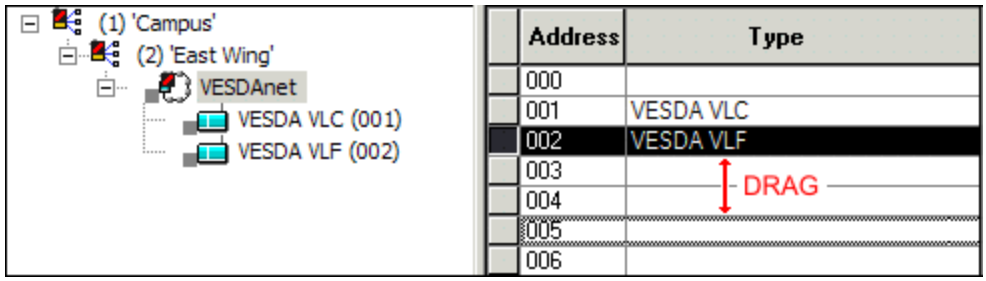


Figure 3-4: Assign Detector Address (VESDAnet shown)

Once this has been done then the Designer should edit the network connection properties. The Connection tab will allow the designer to define the connection that VSM4 will use to connect the network via a real HLI (VESDAnet) or an RS485-RS232 converter (MODBUS RS485). The Browse button on the dialog will bring up the Connection Manager which displays all defined connections and also provides wizards to guide the designer in defining new connections. These are described further in Appendix D.

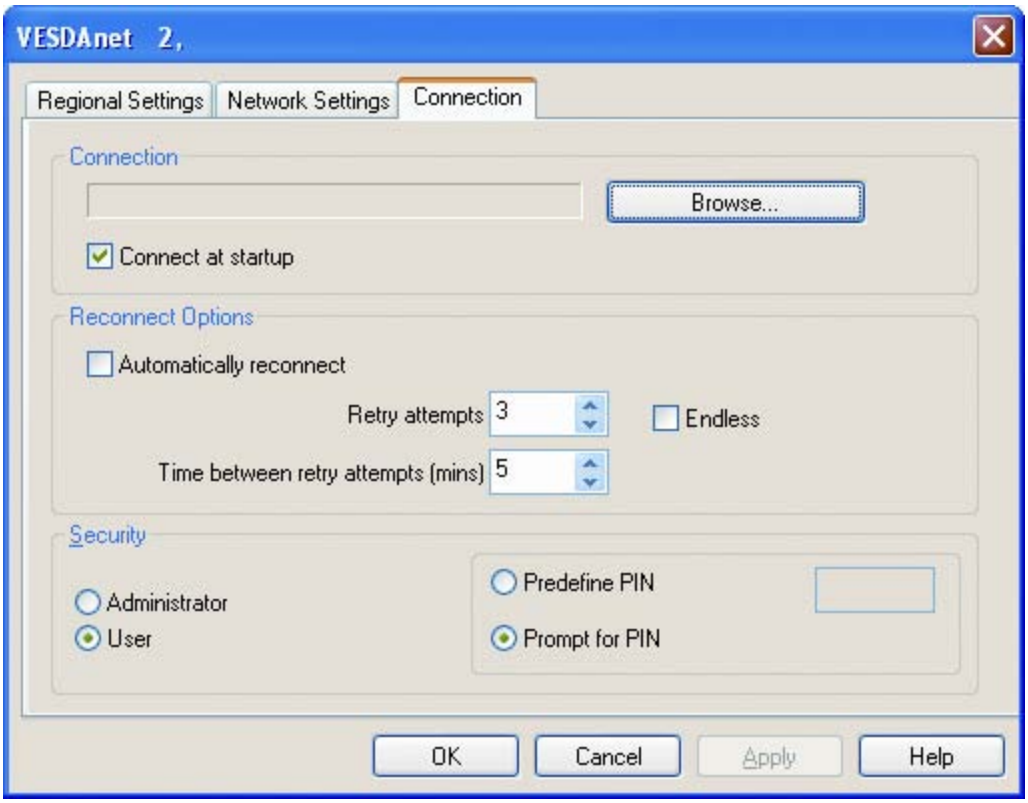


Figure 3-5: Connection Tab for VESDAnet or MODBUS RS-485 networks

The connection tab also allows the automatic reconnection rules to be defined and allows the Designer to predefine the specific access PINs for this connection. It is recommended that the Designer define all the PINs up to Administrator level.

Once the Connection has been defined then the Designer can click on the **Connect and Synchronize** toolbar button (if there is access to the real system) to connect to this network.

Similarly, connections need to be defined for all the other networks that are to be monitored. Once this is done then the structure should be saved.

Note: All networks should be directly connected into the logical structure. This ensures that VSM4 can send configuration and retrieve event log data.

3.1.2 Building the Floor Plans

Now that there is a logical structure that integrates all devices in all of the monitored networks, the location structure must be defined. This structure defines a hierarchy of geographical regions.

A typical floor plan hierarchy would consist of:

- a geographical map of the site with all buildings (top level of hierarchy) marked up
- aerial map of each building
- elevation view of each building
- floor plan of each building level

There are no bounds on the logical hierarchy that can be built.

Note: It is the Floor Plan view that most operators will use to navigate around the fire system, since it provides a visual representation of the buildings and regions that are being protected by the fire detection system.

To create a new Floor Plan

1. Log on as the Designer.
2. Select **View > Floor Plan** from the menu system. The screen divides into two panes, the upper showing the monitoring structure, the lower showing the Floor Plan.
   Note: It is also possible to open a blank Floor Plan by selecting **File > New > Location**. If this method is used, the Floor Plan file must be the saved with the same name as the Monitoring Site.
3. Select **Floor Plan > Designer Mode** from the menu system. This allows you to modify the Floor Plan.

Often the top levels of the Location structure are based on images such as maps or aerial photos of sites. As the Location structure is built, the locations should be edited and given meaningful names and abbreviations. The Floor Plan tab should be used to define the background image or CAD drawing. Use the **Import…** button (see below) to browse to the image or CAD file.

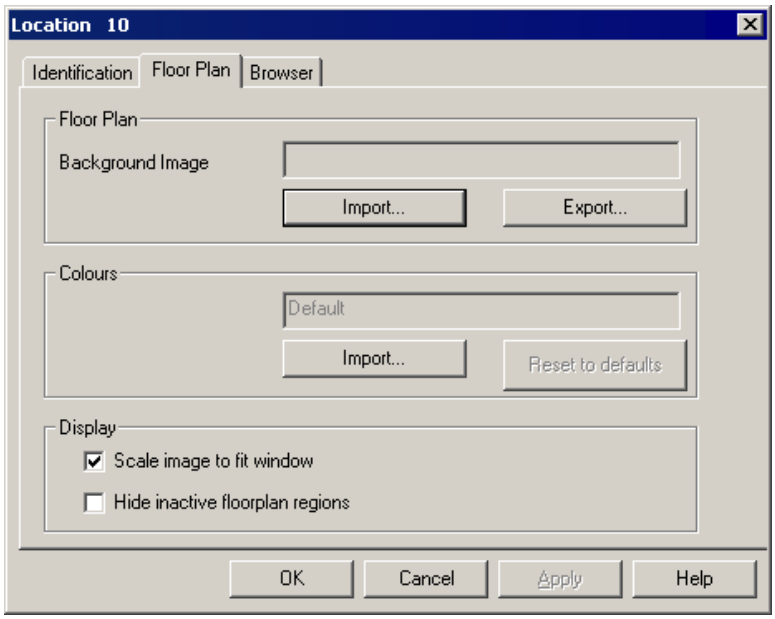


Figure 3-6: Location Properties - Floor Plan Tab

Where possible, use Vector graphic image files as they allow maps and Floor Plan drawings to be enlarged and reduced without losing image quality. Vector drawings include files with these extensions: *.cgm, *.dwg, *.dxf, *.emf, *.vec and *.wmf.

When using CAD files, minimize fine building details, as this will affect application performance. The detail should be just sufficient to clearly indicate fire zones and locations of devices. In general, keep file sizes below 1MB.

Note: The **Insert > Image** on the context menu on the floor plan (right side) partition should never be used for background images. It is used to add annotations into a Floor Plan file.

Structure of a Floor Plan Location

The Floor Plan that is associated with each location has a layered structure where the imported background drawing or image is at a lower layer and then regions associated with zones and detectors are placed in a special upper layer. The Import button on the Floor Plan tab imports the background image or drawing to the lower layer.

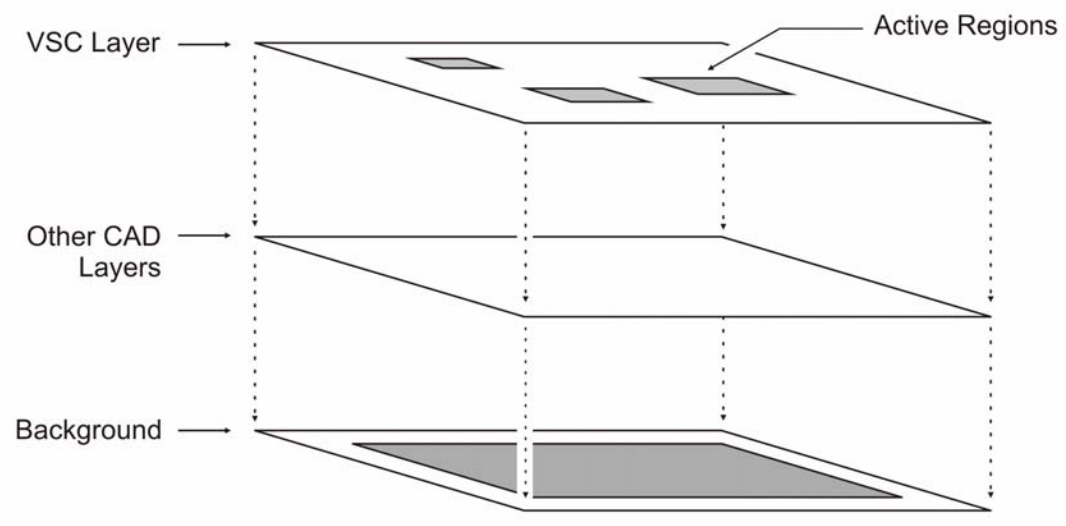


Figure 3-7: CAD Layering

The Insert sub-menu options on the floor plan context menu are used to create regions in the upper VSC layer.

Setting up Hyperlinks

Adding a hyperlink involves creating a region on the floor plan, using the **Insert** context menu, then dragging a device (usually a detector) from the Monitoring Structure onto that region.

A hyperlink to another location can be created in the same way by dragging another node in the floor plan tree and dropping it on a pre-defined region. As each hyperlink is created, an item is placed in the tree. By default the name and properties of that item will reflect those of the device (or location) to which they are linked. However, the name can be edited if the designer wishes to use a different name. This is particularly useful to give VLS sectors distinct names.

Note: Setting up the hyperlinks is best performed while in offline mode. This avoids potential interference from faults, alarms and other events, and also provides the ability to do the work offsite. To work offline, simply disconnect from any networks.

Save the Floor Plan

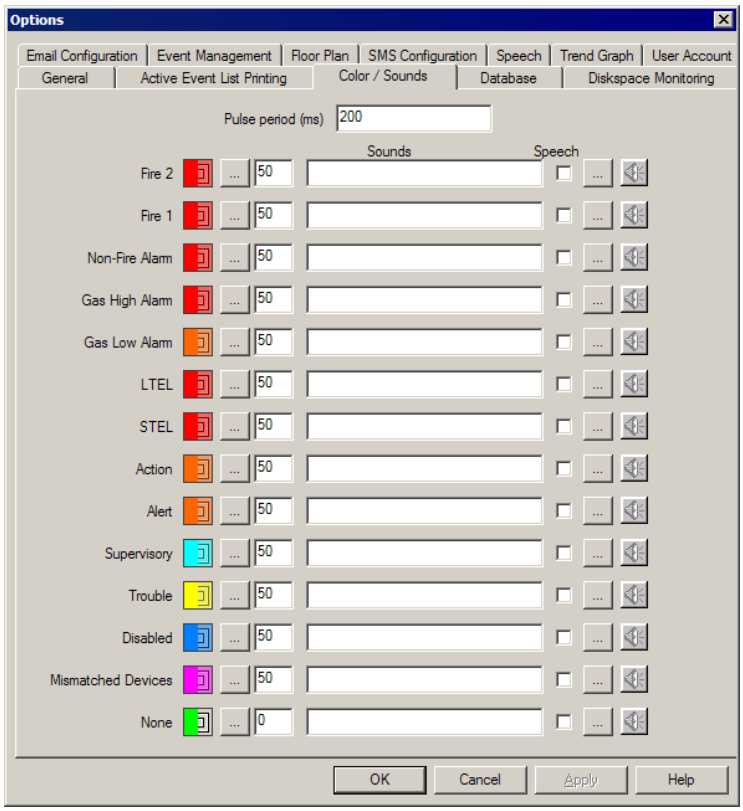
1. Select the Floor Plan.
2. Select **Save** from the Toolbar.
3. If prompted, enter a file name for the Floor Plan. It should be the same as the file name for the Monitoring Site. The .vfp file extension will be automatically added.
4. Change from Design Mode back to Monitoring Mode by selecting **Floor Plan > Monitor Mode**.

3.1.3 Customize the Status Bar

The Status Bar, located at the bottom of the main screen, shows the highest priority event in the system. The color of the bar reflects the event type and a custom sound or speech can be generated. The customization of the color also affects the zone displays on the floor plan.

Colors and Sounds Options

The Color/Sounds tab of the Options dialog (Figure 3-8) is used to set the color and sound parameters for each type of event. This affects the background color in the Active Event List, Event Log and Status Bar, and the zone region in the Floor Plan.



Setting	Description
	Blue, 0% Opacity
	Blue, 50% Opacity
	Blue, 100% Opacity

Button	Description
...	Browse. If Speech is licensed, this will open the Speech Edit dialog, otherwise it will open the file dialog.
	Play Sound through Speakers

Figure 3-8: View > Options > Color / Sounds

The color and sound settings are as follows:

- **Pulse Period -** The rate at which the indicators flash in the Alarm Status Tab of the Status view. This also sets the rate of flashing for the Zone in the Floor Plan.
- **Color Selection -** A color is assigned to each event type. Select the corresponding browse button to open the color picker and change the color.

- **Opacity -** The opacity of the selected color in the textbox. Enter a value between 0 (transparent) and 100 (fully opaque).
- **Sounds -** A wav format sound file can be assigned to each event type. The sound will play when an event of that type is received. Select the corresponding browse button to select or change the sound file.
- **Speech -** If the Speech checkbox is ticked, the Customize Speech dialog is displayed when the browse button is selected. Use this dialog to change the words and sounds used in a spoken message. Note that this option is only available when the Text-to-Speech feature has been licensed.
- **Sample -** To listen to the selected sound, select the speaker button.

3.1.4 Customizing Speech

The Customize Speech dialog allows the user to define a template that combines both speech and pre-recorded sounds like bells and whoops.

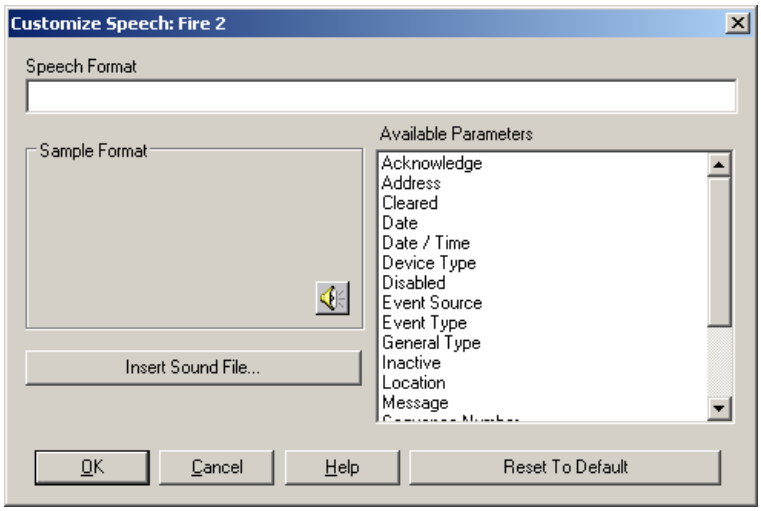


Figure 3-9: Customize Speech

The top edit field represents the template with literal text shown in black and placeholders for event fields shown in blue. Literal text can be directly entered and edited. Placeholders are entered by selecting the field in the list and then clicking on the Insert button. The placeholder will be inserted where the cursor is in the edit field. They can be removed by selecting the placeholder and hitting **Delete**. Pre-recorded sounds are inserted by clicking on the **Insert Sound File** button. To listen to the template, as applied to a sample event, click on the speaker button.

Speech Options

The Speech tab of the Options dialog (Figure 3-10) is used to set the parameters for the use of the optional Text-to-Speech feature (refer to section 2.3.1 for further information).

Note: Speech must also be enabled for specific event types in the Colors / Sounds tab. Refer to section for further information.

Edit Speech Options

1. Select **View > Options** > Speech from the menu system.
2. Edit settings as appropriate.

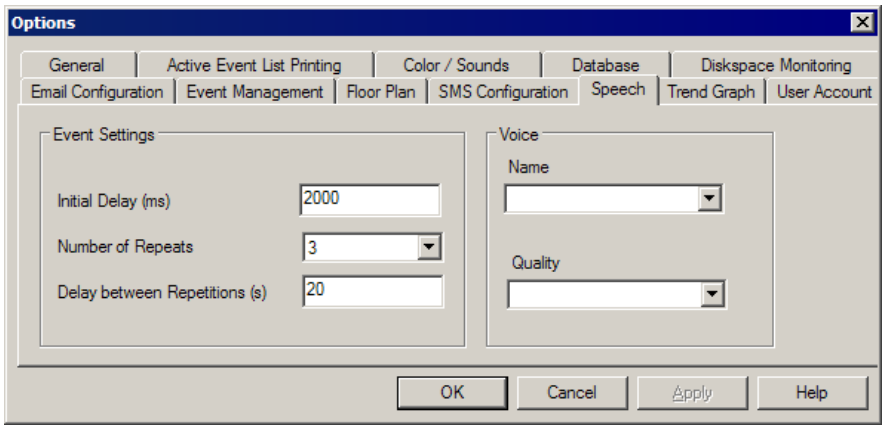


Figure 3-10: View > Options > Speech

Event Settings

- **Initial Delay -** The delay in milliseconds between VSM4 receiving an event notification and it being annunciated. This avoids having partial messages interrupt each other where several messages are received together.
- **Number of Repeats -** The number of times an event notification is repeated.
- **Delay between repetitions -** The delay in seconds between each repeat of the notification.

Voice

- **Name -** Select the name of the voice and language used to deliver the notification from the drop down.
- **Quality -** Select the sound quality of the notification from the drop down menu. There is usually no need to choose anything other than full quality.

These drop-downs will be empty if no Text-to-Speech language packs have been installed. Refer to section 2.3.1 for further information.

3.1.5 Define Responses

VSM4 supports linking response documentation to zones, thus providing instant context-relevant information to the operator when an incident occurs. This can warn the operator of specific dangers associated with an area, such as the presence of dangerous chemicals or it can remind them of standard site operating procedures. The Designer will usually take documentation associated with locations and condition responses provided by the end user and link these into the Floor Plan structure that has been created.

Documents that detail response procedures can be linked to specific locations and customized for specific event types. Any HTML page that can be viewed in Microsoft Internet Explorer can be used by VSM4. Many modern document authoring applications can export documents to HTML. It is also possible to link to animated HTML pages or even to web cameras.

General Responses

VSM4 allows the Designer to define responses specific to a given location and event type while also allowing the Designer to specify general policies and procedures.

During monitoring, the HTML documents are displayed in response to the events that they are linked to. If there is a HTML page defined for the event and its location then it is used. However, if there isn't a specific URL for the event type/device combination then the parents of the device in the Floor Plan are checked for a URL of the same event type. If no match is found there then the parent's parent is checked until a match is found or the top of the tree is reached.

Each event type can refer to separate documents, or if the complexity of the site does not require a lot of detail for each procedure, all procedures can be placed on a single document. Advanced users

can then utilize bookmarks to open the document to a specific location within the overall document for each event type.

Response Content

Expected event responses are:

- **Fire events -** should describe evacuation procedures and the locations of hazards.
- **Supervisory and Trouble events -** contact details for a sufficiently trained person in order to diagnose and correct a fault or carry out the required process, for example a filter change.

Response Definition Procedure

To associate Procedure Documents with Floor Plan elements:

1. Log in as the Designer User.
2. Open the Floor Plan and select **Floor Plan > Designer Mode**.
3. Right-click over any item listed in the Floor Plan, select **Edit** from the context menu and then the Browser tab.
4. Enter a file location or an internet address (URL) for each event type (refer to Figure 3-11 below).

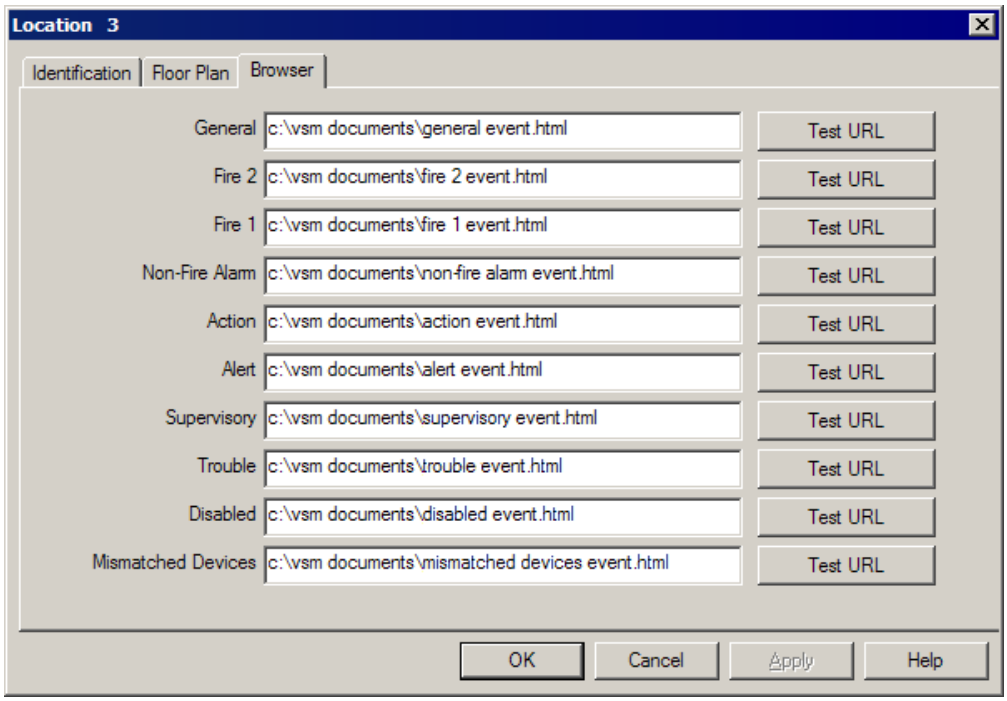


Figure 3-11: Edit Location: Document Event Type Assignment

5. Select **Test URL** to ensure that VSM4 can read the document correctly. The browser view must already be open to enable this to work correctly.

3.2 Remote Notification

The Remote Notification system is an optional feature that enables reporting of specific events to remote users by email or SMS.

Examples of use are:

- to notify a building manager of a pre-alarm so that it can be checked and possibly dealt with, avoiding a fire brigade call out.
- to notify a maintenance manager of urgent faults that require attention.

Designer or administrative level access is required in order to configure Remote Notifications, but any user can receive them.

Prerequisites

Prior to defining remote notifications, the ability for VSM4 to send an email or SMS must be configured:

- Email Server - The email server configuration must be entered and tested. Select **View > Options > Email Configuration**. Refer to section .
- Email Addresses and Telephone Numbers in User Accounts - Each user that is to receive notifications must have a local VSM4 user account with a valid email address that has been specified in the User Manager (**Security > Manage Users**). Refer to section 6.1.4 for further information on user accounts.
- GSM Modem - The configuration for the modem must be entered and tested. Select **View > Options > SMS Configuration**. Refer to section .

3.2.1 Notification Specification Configuration (What and Who)

A Notification Specification defines what conditions are to be reported and who should be notified. The Remote Notification Specification may be found by selecting **Monitoring > Remote Notification**.

Add a new Notification Specification by selecting the **Add** button. The Remote Notification specification is displayed (see below).

The upper section of this dialog defines *WHAT* is being reported and the Notification Groups, down the bottom, define *WHO* will be contacted.

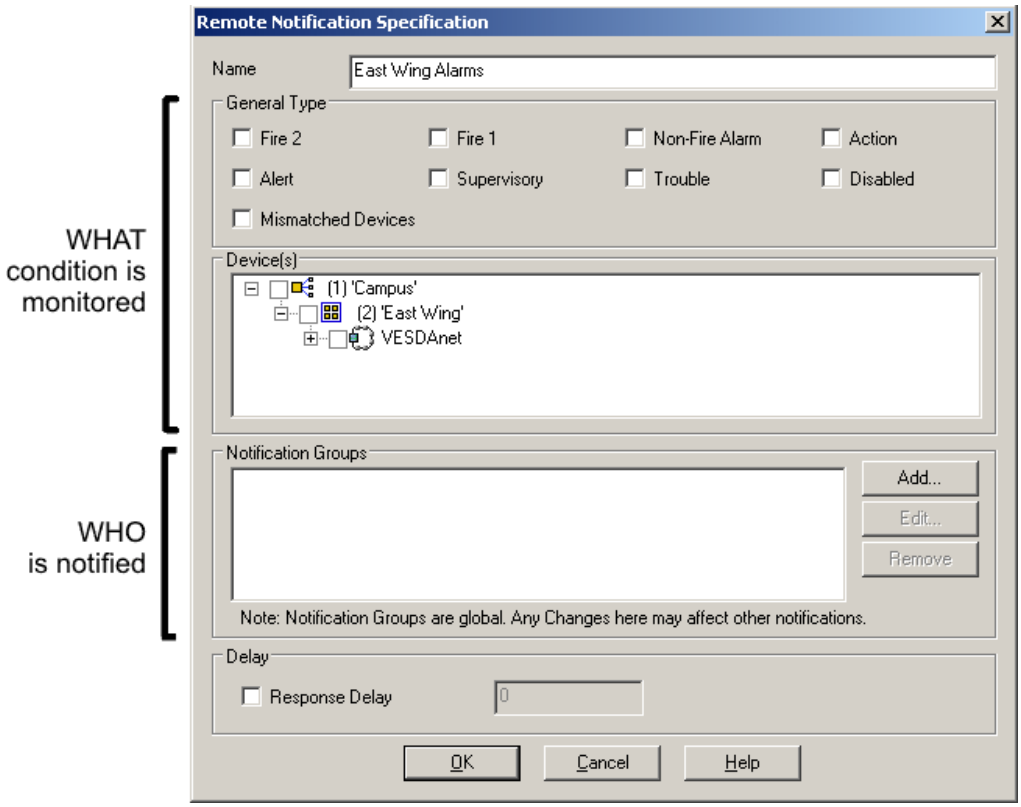


Figure 3-12: Remote Notification Specification

1. Enter a name for this Notification type into the name field. This name allow this notification to be clearly recognized. For example 'East Wing Alarms' may be used for a notification that only responds to alarms in the East Wing of the Campus.
2. Select the event types that trigger the notification, located in the General Type section, by clicking on the check box next to each event.
3. Define the relevant regions by selecting devices that monitor that region. The Monitored structure is shown in the Devices section. Clicking in the box next to a node in the tree will select that node and all of its child nodes. Hence if the entire Monitoring Site was monitoring the East Wing then the site node would be checked which would in turn select all of the detectors and other devices in the structure.

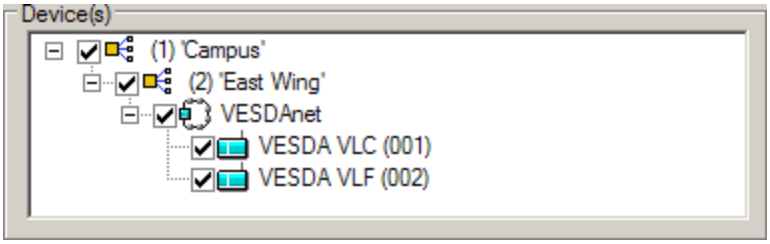


Figure 3-13: All subordinate devices selected by selecting East Wing

Clicking on child nodes allows their state to be reversed so that in the example below the Local Contact Outputs and User Zones are ignored. This could occur if these units were being used to monitor an adjacent wing. When child devices are overridden then the parent's check boxes are grayed so that even when the tree is collapsed the designer can know that child devices are overriding the parent state.

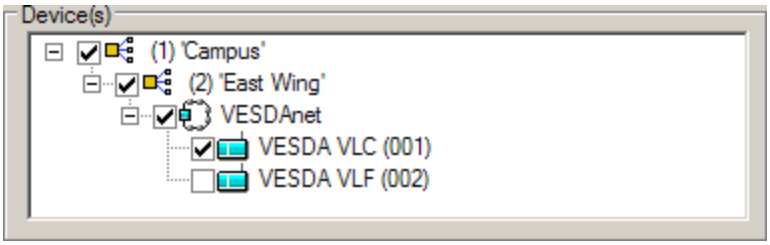


Figure 3-14: Some child devices de-selected

At this stage the triggering conditions are defined and the notification group settings will define who will be notified.

4. Define *WHO* will be notified by selecting one or more Notification Groups by clicking in the box next to the Notification Group name. Refer to section 3.2.2 below for information on adding new Notification Groups.

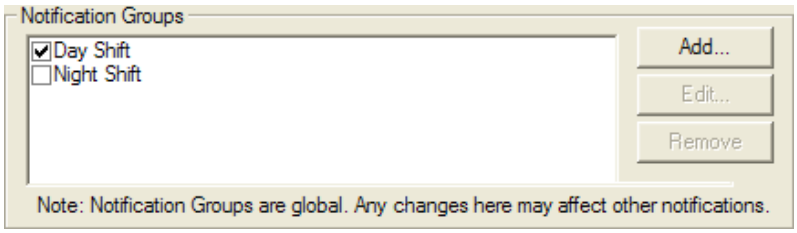


Figure 3-15: Select Notification Group

5. Select the **Response Delay** option and enter a value for the delay period.
This value is the period of time that an event must remain active (not acknowledged, cleared or inactive) before the notification will be sent, and is set in seconds.
This allows the system to avoid sending notifications for transient conditions. For example, opening the door to a computer room may result in an airflow fault on the detector that is protecting the computer room. The fault will disappear as soon as the computer is closed. Setting the Response Delay to a value such as 15 seconds will prevent unnecessary remote notifications from being sent every time someone opens the door.

   The maximum delay is 2419200 seconds (28 days).

3.2.2 Notification Group Configuration

Notification Groups are collections of people with similar responsibilities and work patterns. Often these will correspond to work shifts. Once the group has been created in one Notification Specification, all other Notification Specifications can use it.

Notification Groups allow staff changes to be treated separately from the main notification logic. For example if an operator were to change from a day to a night shift then the notification groups would be changed but the notification specifications would not be affected.

Management tools include adding, editing and deleting of Notification Groups.

To add a Notification Group

1. Select **Add**, located to the right of the Notification Group list (refer to Figure 3-15).

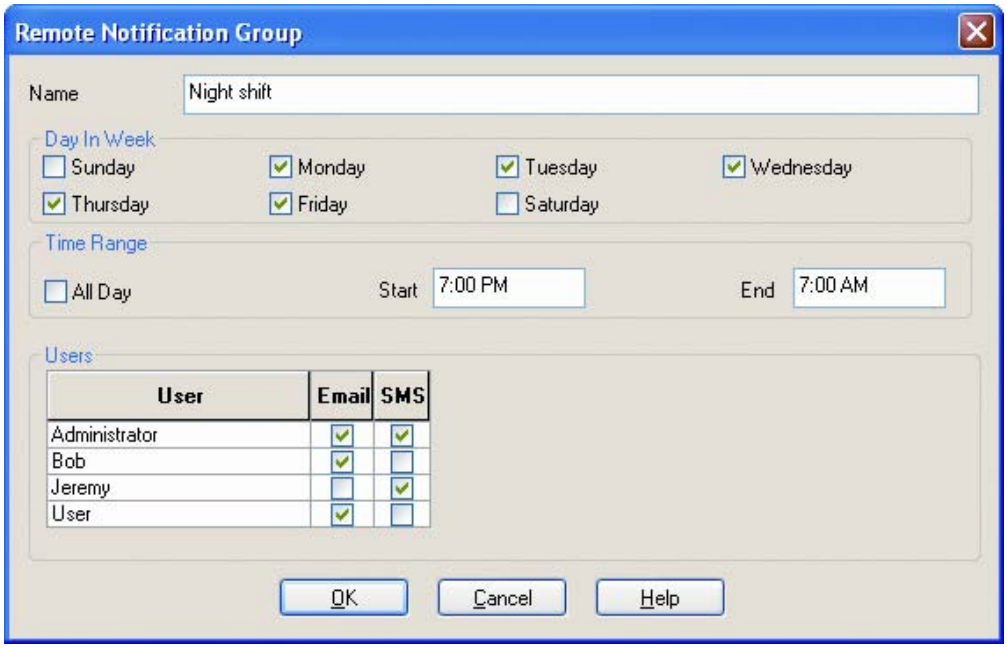


Figure 3-16: Remote Notification Group Editor

2. Enter a name for the group.
   Names would ideally include the main focus of the notification. For example, create a group consisting of all the Weekly Night Shift users.
3. Select which days of the week that the notification group is to receive the notifications.
   For the example, select only the working days and leave the weekends unchecked.
4. Define the time range.
   For example, the night shift would range from 7:00pm to 7:00am.
5. Select which users belong to this group.
   Create new user accounts as necessary (refer to section 6.1.4 for further information). If the user requires no access to VSM4 apart from this notification then they can be given the 'No Access' access.

3.2.3 Notification Mechanism Configuration

Remote Notifications could use a variety of mechanisms to report an event to a remote user. Currently, only emails are explicitly supported. This section describes how to define templates for the automatically generated emails. That is, it defines what information is sent out.

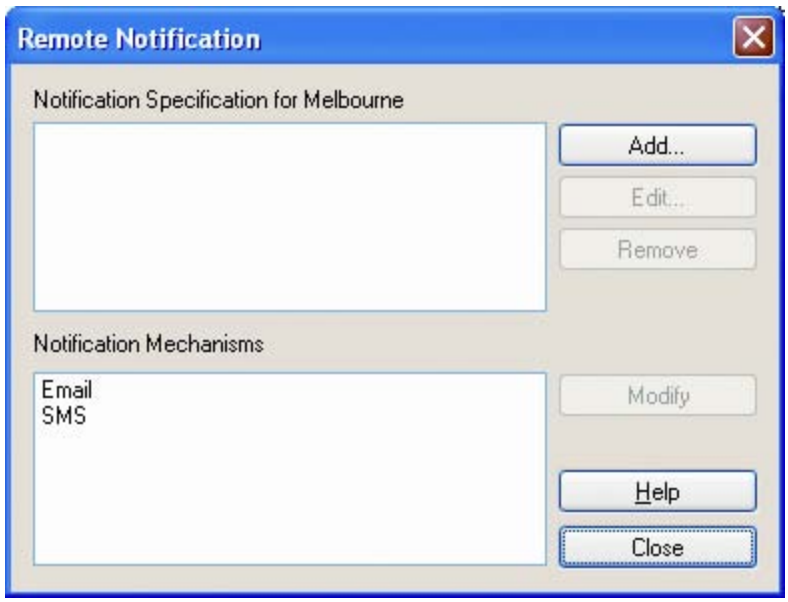


Figure 3-17: Remote Notification Manager

Select Email notification on the Notification Mechanisms dialog, then click the Modify button, to define the templates. The Email Format Configuration dialog box is displayed (see Figure 3-18 below). It lists all the active event categories on the left. Each of these can have a specialized template defined since different event categories may need to convey different information. For example, a Trouble event would normally contain a trouble ID which would be meaningless for an Alarm event.

Selecting an event category on the left displays its template on the right panel where it can be edited. The tool allows both the subject and body of the email to be built up of literal text and event fields. The literal text is shown in black and is directly edited. This has been used to create labels in the example.

The fields show up in blue and are added by positioning the cursor where needed and clicking on the parameter in the Available Parameters list on the right-hand side. They are deleted by selecting the field and hitting delete. They can't be otherwise edited. To populate the template, any item from a list of dynamic parameters can be combined with free text in the mail subject and body.

The Email Sample tab shows the effect of applying the template to a typical event.

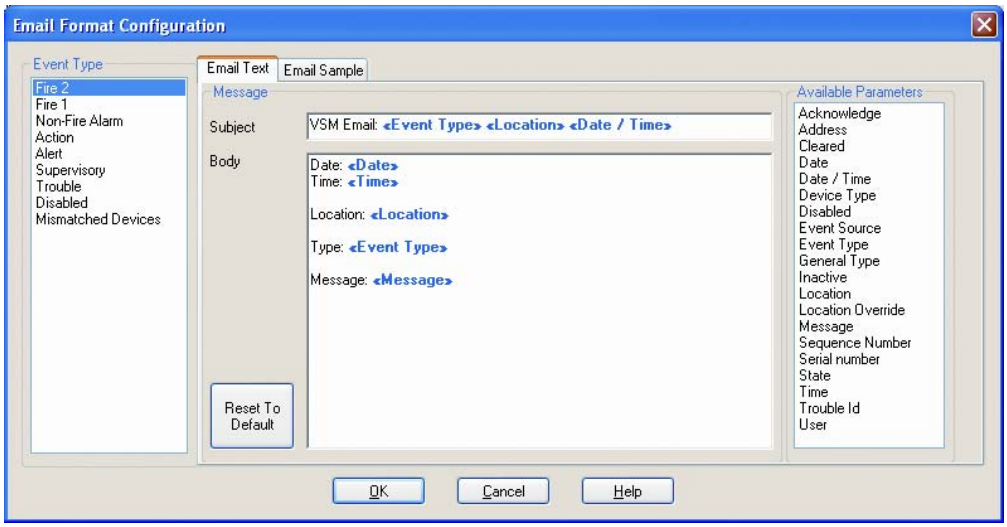


Figure 3-18: Email Format Configuration

Note: Formatting functions are not available (e.g. bold, italic, colors), however it is possible to use html to achieve this if the recipient has an HTML compatible email client. Detailed information on this is beyond the scope of this document.

Email Configuration Options

The Email Configuration Tab of the Options dialog (Figure 3-19) is used to set email server options for the optional Remote Notification feature.

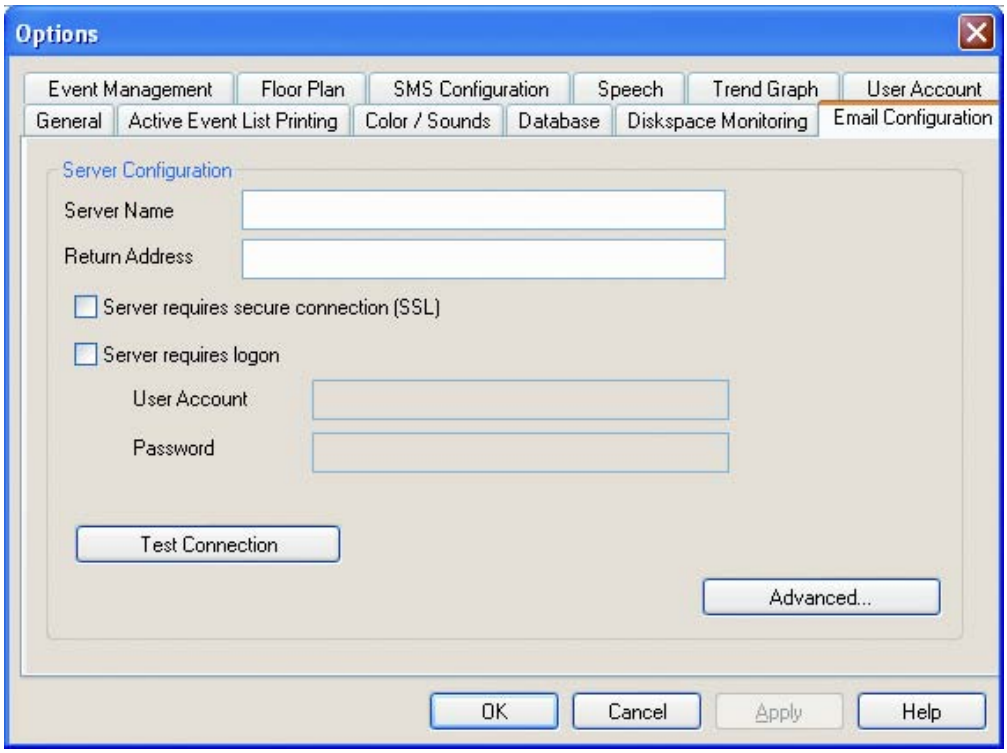


Figure 3-19: View > Options > Email Configuration

Note: In order for the Remote Notification system to be able to send notification emails, it is necessary to either have a valid account on an email server that is permanently accessible to the Monitoring Computer, or if one is not available to install an email server application on the Monitoring Computer. Consult with your IT administrator to determine the appropriate option and obtain the required settings.

Email Configuration Settings

- **Server Name -** The domain name, network name or IP address of the email server that will send the notification emails.
- **Return Address -** The email address that will appear as the return address in the notification emails.
- **Server Requires Secure Connection -** Select for mail servers that use SSL encryption. If this is required, the information will be provided to you with your mail account details.
- **Server Requires Logon -** This may be required if the mail server software is not installed on the Monitoring Computer. Use the username and password provided with your mail account details.
- **Test Connection -** Test that the access information to the mail server has been correctly entered by initiating a connection.
- **Advanced -** This setting allows selection of a non-standard outbound email port and alternate login method. The default email port setting is Port 25 for standard and Port 443 for SSL.

SMS Configuration Options

The SMS Configuration Tab of the Options dialog (Figure 3-20) is used to set the GSM Modem communication settings for the optional Remote Notification by SMS feature.

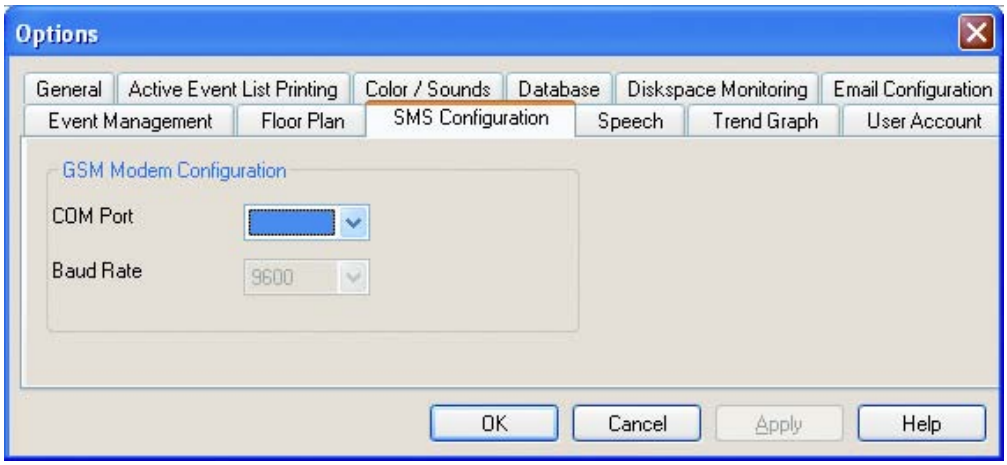


Figure 3-20: View > Options > SMS Configuration

SMS Configuration Settings

- **COM Port -** The COM Port on the PC that is connected to the GSM Modem for sending SMS notifications.
- **Baud Rate -** The baud rate for communicating with the GSM Modem.

3.3 Verification

Now that the monitoring site has been described and event responses defined the structure should be verified.

The first step is to run the Verification tool which will scan the structure and report logical inconsistencies.

1. Select a node on the Monitoring Structure.
2. Invoke the verification tool using **Edit > Verify** menu. Any errors or warnings will be displayed on the Verification dialog.

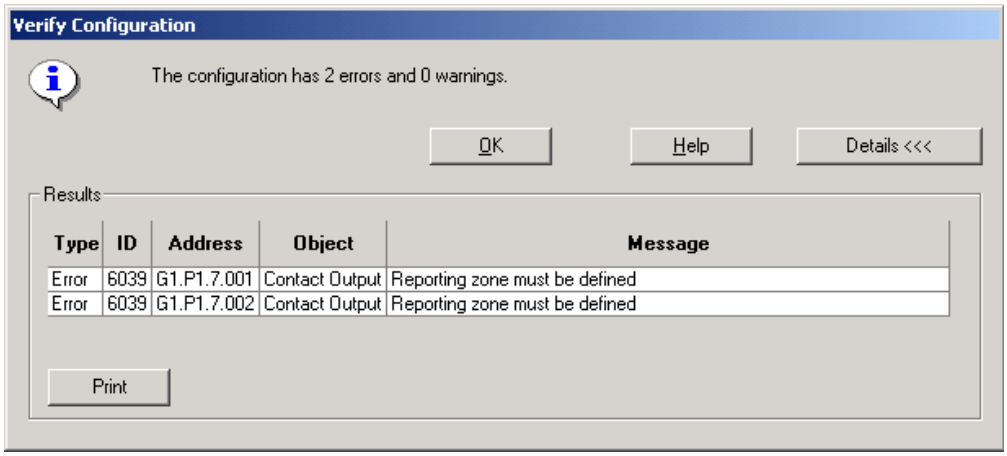

Verify Configuration
The configuration has 2 errors and 0 warnings.
OK
Help
Details <<<
Results
Type ID Address Object Message
Error 6039 G1.P1.7.001 Contact Output Reporting zone must be defined
Error 6039 G1.P1.7.002 Contact Output Reporting zone must be defined
Print

Figure 3-21: Verify Configuration

The errors indicate missing information or inconsistencies that must be addressed. The warnings indicate unusual or potentially dangerous settings that may be due to an oversight and so should be reviewed. These errors and warnings apply only to the Monitoring Structure.

3. Select a node in the Floor Plan tree.
4. Invoke the verification tool using **Edit > Verify** menu. Any errors or warnings will be displayed on the Verification dialog. The errors and warnings will apply to the Floor Plan structure and the Monitoring Structure.

Once the logic in the monitoring structure and floor plan has been verified then the following should be tested.:

- All connections work reliably.
- All networks and detectors have been included in the Monitoring Structure and Floor Plan and associated correctly. If there are missing detectors, that is detectors assumed in configuration but not reported by the VESDAnet, then these will be reported as missing device troubles on the Active Event List. If detectors are not represented on the Floor Plan then warnings will be reported by the Verification tool.
- All procedure documents open correctly in the html browser view. To test this select each node in the Floor Plan tree that has associated documentation and click on the Test button for each documented event type.
- All remote notification mechanisms operate as expected. The simplest way to test this is to run Alarm tests on detectors and check that notifications are received by all relevant staff.

3.4 Events

3.4.1 Event Log Database Configuration

VSM4 can be configured to continuously log VESDAnet and standalone detector events to a specified database. This allows a much longer history of events to be maintained than is provided by an individual onboard event log and allows events from all of these devices to be integrated. Application events such as when operators log on and off the system can be recorded to the database and viewed along with device events.

The Primary instance of VSM4 is responsible for retrieving events from each monitored detector and writing them to the assigned database. A Secondary instance of VSM4 can read events from the database, but cannot write device events to the database.

When monitoring a network using multiple computers, one should be set to primary and all others should be set to secondary. The secondary computers should all be set to view the database where the primary computer is storing the device events.

It is possible to define a different database at any logical node in the monitoring structure, however, it is recommended that the same database be used for all devices and application events (if using a primary monitoring computer).

Event Logging is configured by using the Event Logging property page for a Monitoring Site or Logical Node. This requires Administrator-level access and is only possible when VSM4 has been started in primary mode (refer to section 2.2.3).

Database Selection

It is possible to use a VSM Managed database or to connect to an existing SQLite or ODBC compliant database. The VSM Managed database option is enabled by default.

To use a VSM Managed database

1. Double-click on Monitoring Site or Logical node and select the **Event Logging** tab (Figure 3-22).
2. Select VSM Managed.
3. Select **Apply**.

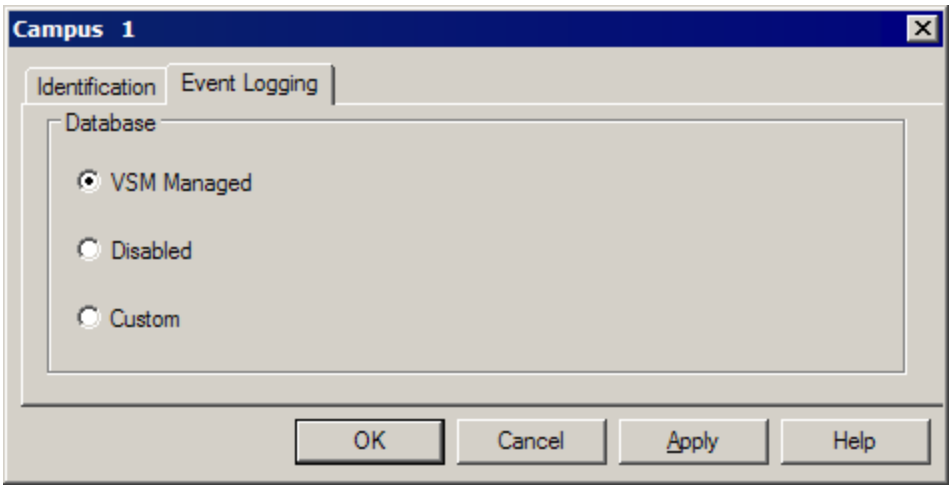


Figure 3-22: Event Logging Configuration

To select an existing custom database (Primary and Secondary)

1. In the Event Logging Configuration tab (Figure 3-22), select the **Custom** option and then the Select button.
2. Select an existing database from the list of available databases (Figure 3-23).
3. Click **OK**.

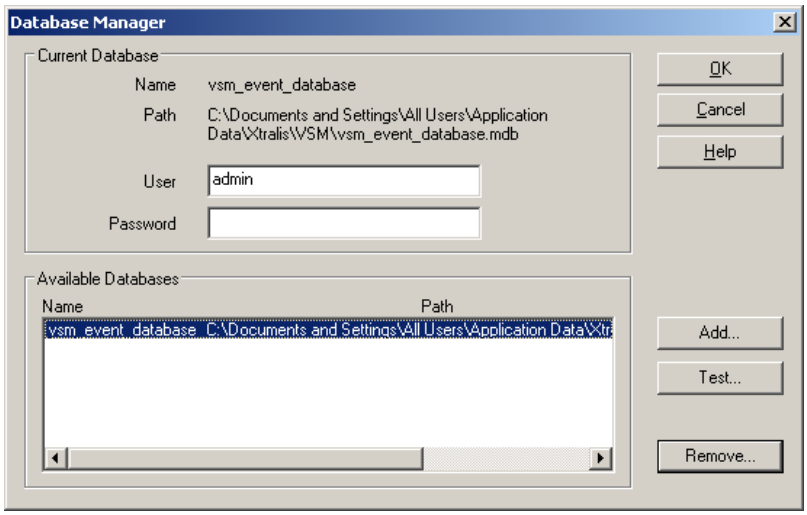


Figure 3-23: Event Database Manager

To create an SQLite database

1. Select the **Select** button.
2. Select **Add** (Figure 3-23).

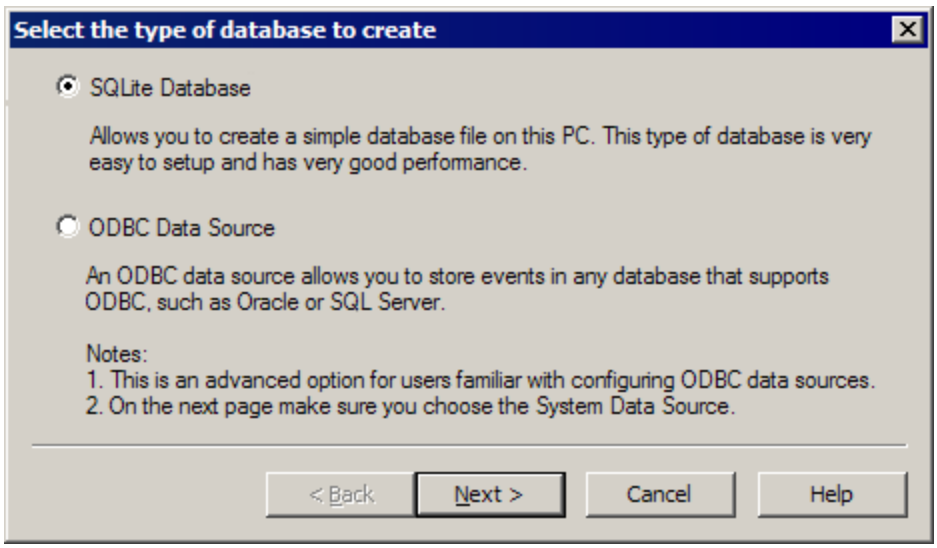

Select the type of database to create
SQLite Database
Allows you to create a simple database file on this PC. This type of database is very easy to setup and has very good performance.
ODBC Data Source
An ODBC data source allows you to store events in any database that supports ODBC, such as Oracle or SQL Server.
Notes:
1. This is an advanced option for users familiar with configuring ODBC data sources.
2. On the next page make sure you choose the System Data Source.
< Back
Next >
Cancel
Help

Figure 3-24: Select Database Type (SQLite)

3. Select **Next**.
4. Enter a name for the SQLite database, and select Browse to enter a storage location for it (Figure 3-25).
5. Select **Finish**.

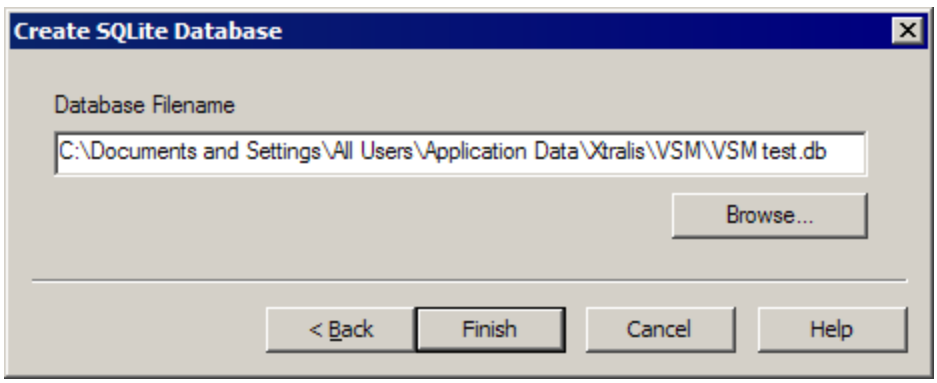


Figure 3-25: Event Database File Name and Location

This database file must be available to the Secondary Monitoring Computer on a shared network drive. If no login name or password was specified, the user name for the database will default to admin.

To create a new ODBC database

Note: Prior to following this procedure, it may be necessary to create a blank database on the main database server, and install ODBC client drivers on the monitoring computer that are compatible with the database software that is to be used. Refer to the IT Checklist in Appendix A for details.

1. Select the **Select** button.
2. Select **Add** (Figure 3-23).

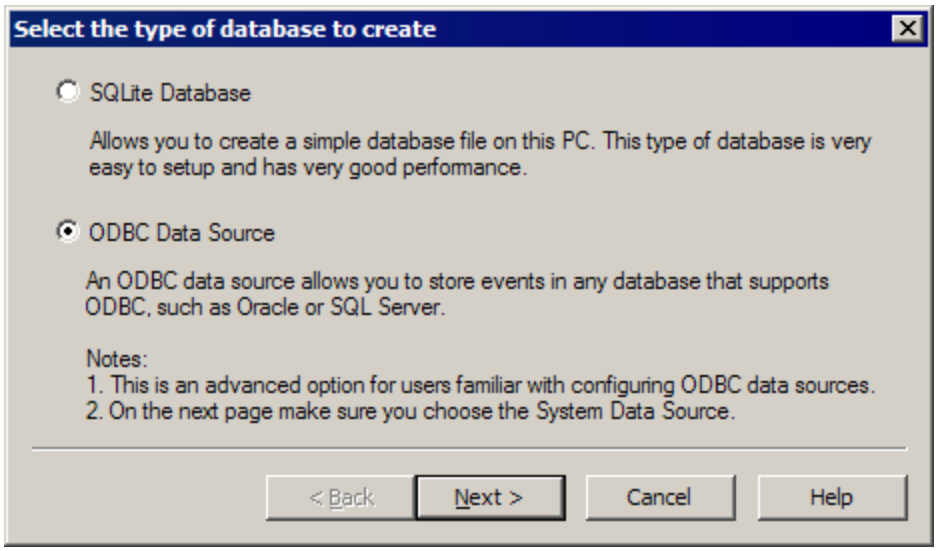

Select the type of database to create
SQLite Database
Allows you to create a simple database file on this PC. This type of database is very easy to setup and has very good performance.
ODBC Data Source
An ODBC data source allows you to store events in any database that supports ODBC, such as Oracle or SQL Server.
Notes:
1. This is an advanced option for users familiar with configuring ODBC data sources.
2. On the next page make sure you choose the System Data Source.
< Back
Next >
Cancel
Help

Figure 3-26: Select Database Type (ODBC)

3. Select ODBC Data Source, then **Next**.
4. Select a Data Source type (Xtralis recommends using a System Data Source):
   - A **System Data Source** can be used by all users on this machine, or by a system-wide service.
   - A **File Data Source** lets you connect with a data source that has file data source names (DSNs). A file-based data source, not necessarily user-dedicated nor local to a computer, can be shared among all users who have the same drivers installed. Select the file data source that describes the driver that you wish to connect to. You can use any file data source that refers to an ODBC driver which is installed on your machine.
   - A **Machine Data Source** is specific to your machine, and cannot be shared. User data sources are specific to a user on this machine, and visible only to that user.

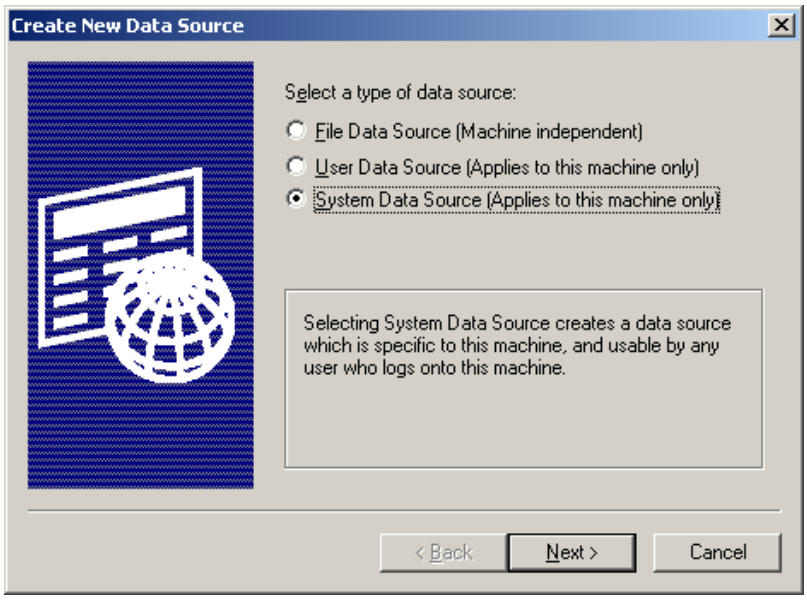

Create New Data Source
Select a type of data source:
File Data Source (Machine independent)
User Data Source (Applies to this machine only)
System Data Source (Applies to this machine only)
Selecting System Data Source creates a data source which is specific to this machine, and usable by any user who logs onto this machine.
< Back
Next >
Cancel

Figure 3-27: Select Type of Data Source

5. Select the correct ODBC driver from the list and select **Next**.
6. Select **Finish**.

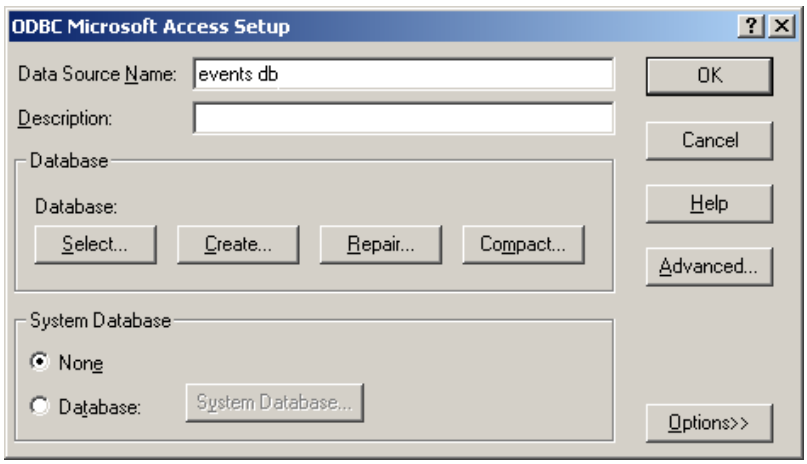


Figure 3-28: ODBC Setup

7. Specify a name for the data source and select a database file using the **Select** or **Create** buttons.

Testing the Database File (Primary)

1. Once you have selected or created a database file, select **Test** to test whether the database was successfully created.

Once connected to a live network and some data has been logged, the **View > Database Event Log** option will become available.

3.4.2 Database Settings

The database which logs system events needs to be setup in a similar way. First, open the Database options tab by selecting the **View > Options…** menu, then configure the following settings:

- **Database -** Select VSM Managed or Custom to set a default database connection, or Disabled to not collect data from compatible detectors and networks.

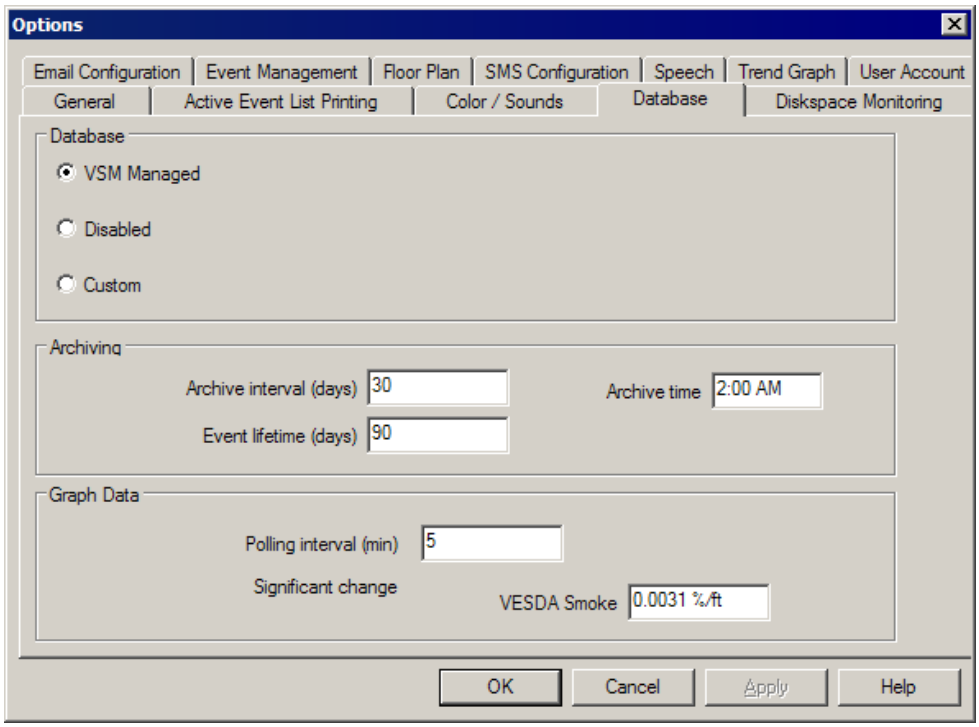


Figure 3-29: View > Database Options

- **Archiving -** these settings determine how often all database logs are archived and purged.
- **Graph Data -** these settings define how significant a smoke change must be before it is logged to the database. A finer setting will increase the detail in historical graphs and may show subtler trends, but it will also increase the volume of data that will be stored.

4 Monitoring

This chapter describes how a typical operator will use VSM4 to monitor a fire system.

In order to be able to monitor a fire system, the software must have been installed and a monitoring structure and floor plans designed as detailed in previous chapters.

4.1 Observation

A typical VSM4 monitoring session would display a Floor Plan view with the status bar at the bottom showing the highest priority condition in the system. The floor plan shows the location of any incidents and provides an intuitive summary of the state of the fire detection system and the buildings. Often a Browser window will also be displayed if the designer has associated procedural or response documents for specific alarm conditions or various regions in the buildings. An example of this layout is shown below in Figure 4-1.

To Start Monitoring

1. Launch VSM4 and open the Floor Plan:
   - Double click a previously prepared desktop shortcut for the Floor Plan (if running in Secondary mode); or
   - Select the **Open** button on the toolbar and select the correct Floor Plan file.
2. Select **View > Browser** to open the Browser view. This displays response procedure documents corresponding to the state of the currently selected region in the floor plan.
3. Resize the views within the same display, or detach and move the new windows to an alternate display (refer to Chapter 6 for further information on working with multiple displays).

The VSM4 screen should now contain the Floor Plan at the top and the Browser in the lower partition as shown below.

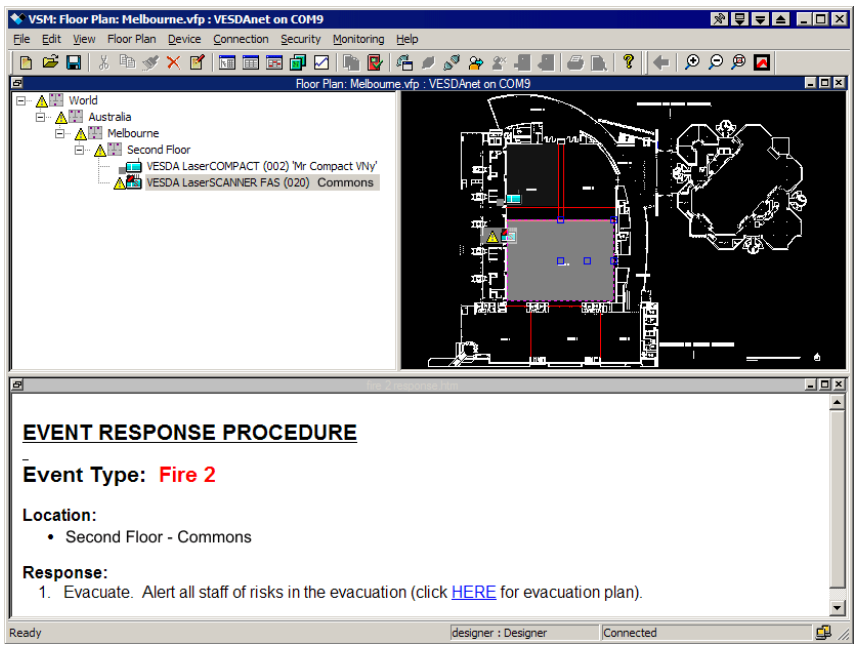

VSM: Floor Plan: Melbourne.vfp : VESDAnet on COM9
File Edit View Floor Plan Device Connection Security Monitoring Help
Floor Plan: Melbourne.vfp : VESDAnet on COM9
World
Australia
Melbourne
Second Floor
VESDA LaserCOMPACT (002) 'Mr Compact VNy'
VESDA LaserSCANNER FAS (020) Commons
EVENT RESPONSE PROCEDURE
Event Type: Fire 2
Location:
Second Floor - Commons
Response:
1. Evacuate. Alert all staff of risks in the evacuation (click HERE for evacuation plan).
Ready
designer : Designer
Connected

Figure 4-1: Recommended Monitoring Arrangement

Note: VSM4 does not currently support saving the workspace layout between restarts. Therefore, it is recommended that the Designer determine the optimum display layout and document this. This will enable monitoring staff to restart the software as necessary and resume monitoring with all necessary information displayed.

4.1.1 Status Bar

The Status Bar always sits at the bottom of the main frame and shows key information about the highest priority condition in the system. Its prominence and simplicity ensure that an operator is made aware of crucial events.

The Status Bar shows the top event on the Active Event List. Refer to section 4.2 for information on the prioritization system that it uses.

Figure 4-2: Status Bar

Contents

The event message sits in the middle of the status bar and is shown in large font. The time-stamp, device type and address appear to the left in normal font. On the right are the Acknowledge, Reset and Silence buttons.

Acknowledge

This button is used to indicate that the user has been made aware of this condition and has acknowledged it. If the event has already been acknowledged then this button is disabled. The status bar will flash while an event is unacknowledged to get the operator's attention.

Reset

Resets the detector which clears events. If the conditions continue to exist then they will be regenerated. This will be disabled if the event relates to a non-detector type trouble such as a 'Lost connection'.

Silence

Silences outputs on the Xtralis VESDA system. This button can be toggled to 'un-silence' a silenced system.

Actions

Double Click

The Status Bar can be configured to respond to a double click by bringing up the Status view or/and causing the Floor Plan view to select the floor plan containing the detector associated with the active event on the status bar.

4.1.2 Floor Plan

The Floor Plan view displays physical locations of where incidents are occurring by associating devices and fire zones with regions on Floor Plans and background images.

An example Floor Plan View is shown in Figure 4-3 (below).

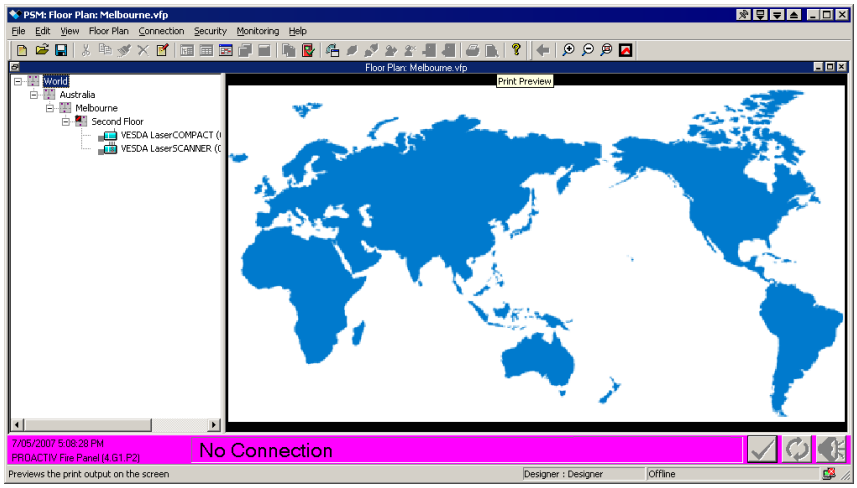


Figure 4-3: Floor Plan View

The Floor Plan can give an overview of the system or can be used to drill down to zones and detectors. Double clicking on an active region will drill down to a more detailed view of the region. The Back menu command (and toolbar button) will step back to the previous view. After drilling all the way down to a device, double clicking will bring up the status view on that device.

Tooltips are shown when the cursor hovers over an active region, providing more information on the target to which the region is linked.

Update Policy

Events propagate up the floor plan hierarchy (i.e. the tree on the left side) so that even when looking at the top most floor plan events on monitored devices on subordinate floor plans are still reported to the operator. A priority system is used when multiple events are active and this is described further in section 4.2.

Locking

The Floor Plans can be configured to always show the location of the highest priority event that is reported on the status bar via the check box on the Floor Plan options shown below. When this option is set it is possible for the operator to override this and prevent the current floor plan from being changed by selecting the **Floor Plan > Locked** menu. This will remain until the operator explicitly disables it or changes to another floor plan.

Display Zoom

There are several menu options that enable the operator to look in detail at a given floor plan. These include:

- basic zoom in/out controls
- a Show All option that optimizes the zoom to just encompass all the image and active regions
- a Zoom previous option that allows the last zoom operation to be undone

Floor Plan Navigator

The Floor Plan Navigator (Figure 4-4) is a tool that provides a resizable overview of the entire image that is currently open in the Floor Plan view, and can be used in both monitoring and design modes. It can be invoked by selecting **Floor Plan > Navigator** or the Navigator button on the toolbar.

The red rectangle in the Navigator represents the area currently shown in the Floor Plan view. When the image has been zoomed, it can be moved around within the navigator to change the area of the image currently being viewed.

The navigator can be resized by left-clicking and dragging the outer border in any direction. The image can be zoomed in or out of by activating the zoom slider or the in/out buttons located at the bottom of the navigator window with the left mouse button.

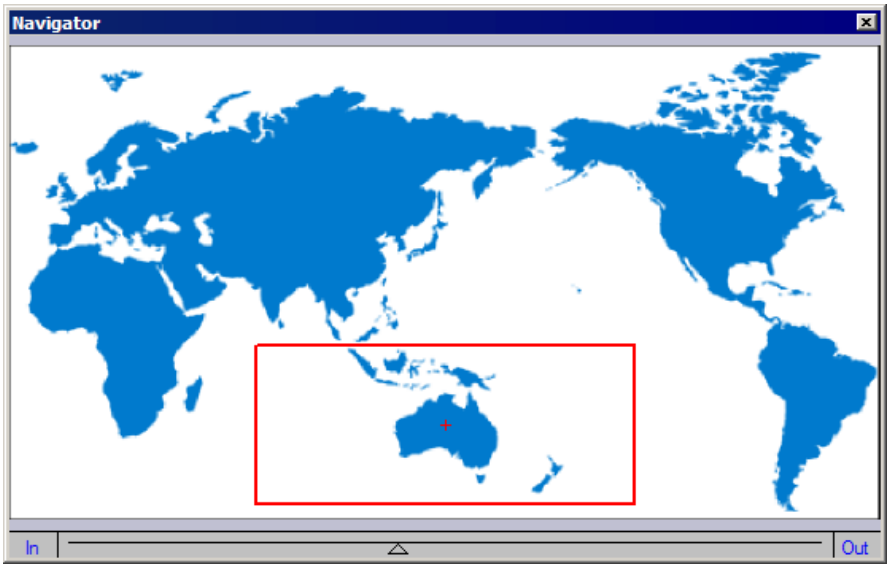


Figure 4-4: Floor Plan Navigator

Toolbar

Toolbar buttons correspond to the Back command, Zoom In, Zoom Out, Show All and the Navigator functions.

Figure 4-5: Floor Plan Navigator Toolbar

Floor Plan Options

The Floor Plan tab of the Options dialog (Figure 4-6) is used to set Floor Plan view behavior and display options.

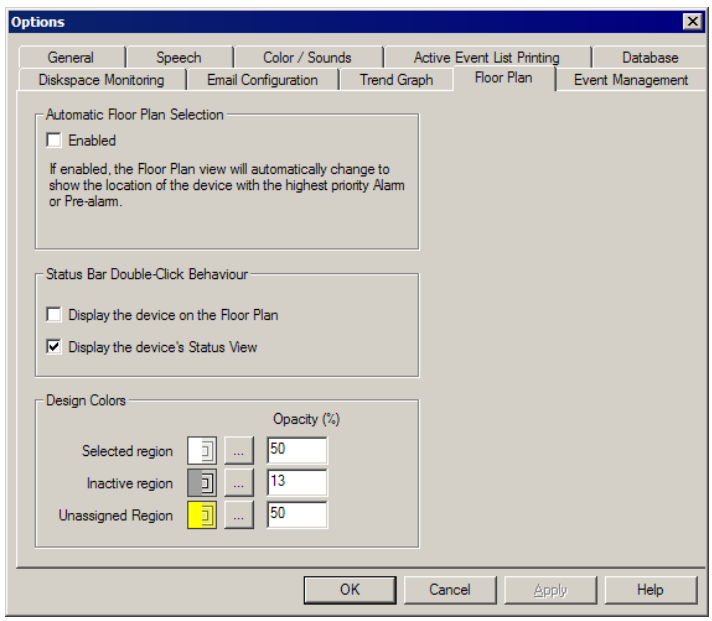


Figure 4-6: View > Options > Floor Plan

Floor Plan Settings

- **Automatic Floor Plan Selection -** When the Automatic Floor Plan selection checkbox is ticked, the Floor Plan automatically changes to show the location of the device with the highest priority Alarm or Pre-Alarm.
- **Status Bar Double-Click Behavior -**
  - If the Display the device on the Floor Plan checkbox is ticked, the device will be displayed on the floor plan when the status bar is double-clicked.
  - If the Display the Device's Status view checkbox is ticked, the device's status view will be displayed when the status bar is double-clicked.

Response Procedures

The Browser shows the user document(s) that describes responses to active conditions in the current floor plan. The content of these documents will usually be provided by the site and integrated with the floor plans by the Designer. The operator should be familiar with these procedures and trained to refer to them when an incident occurs.

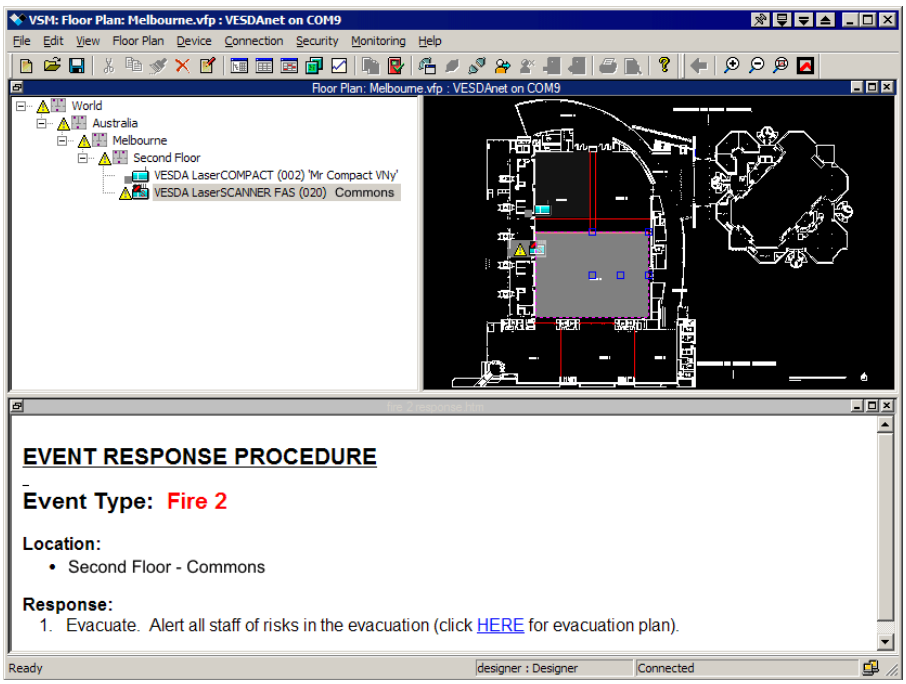

VSM: Floor Plan: Melbourne.vfp : VESDAnet on COM9
File Edit View Floor Plan Device Connection Security Monitoring Help
Floor Plan: Melbourne.vfp : VESDAnet on COM9
World
Australia
Melbourne
Second Floor
VESDA LaserCOMPACT (002) 'Mr Compact VNy'
VESDA LaserSCANNER FAS (020) Commons
EVENT RESPONSE PROCEDURE
Event Type: Fire 2
Location:
Second Floor - Commons
Response:
1. Evacuate. Alert all staff of risks in the evacuation (click HERE for evacuation plan).
Ready
designer : Designer
Connected

Figure 4-7: HTML Browser

4.1.3 Active Event List

The Active Event List provides a prioritized list of all active conditions within the system which serves as a quick summary of the state of the entire system. The alarms and troubles are sorted so that the highest priority conditions appear at the top of the list. An event is considered to be active if it is still current or if latching is enabled and it is waiting for an acknowledgement from the operator.

Active Events are associated with each connection and will automatically be removed when the connection closes. In monitoring systems, an overall Active Event List is used which integrates all conditions from all the live connections, as well as any troubles associated with VSM4 itself.

To display this list, select a node in the floor plan tree and then select **View > Active Event List**, or double-click on the connection icon in the bottom right-hand corner of the VSM4 window. An example Active Event List View is shown in Figure 4-8 below.

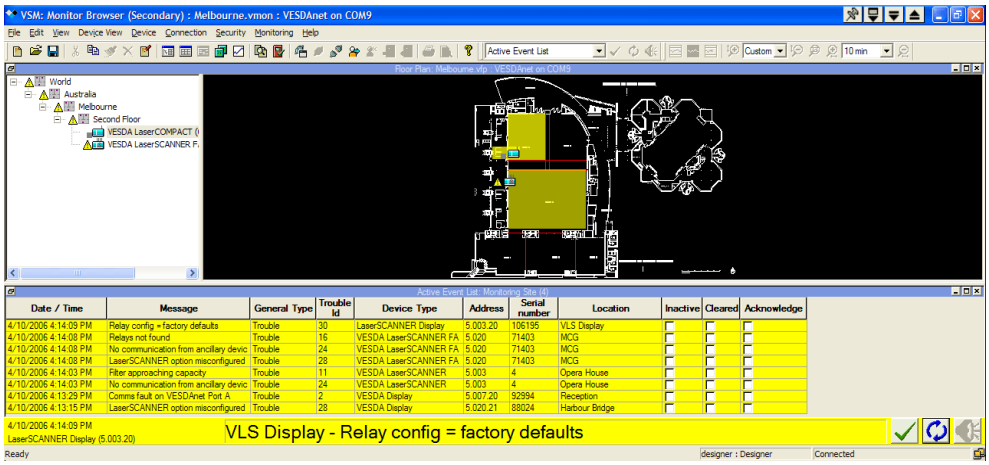

VSM: Monitor Browser (Secondary) : Melbourne.vmon : VESDAnet on COM9
File Edit View Device View Device Connection Security Monitoring Help
Active Event List
World
Australia
Melbourne
Second Floor
VESDA LaserCOMPACT ()
VESDA LaserSCANNER F.
Date / Time | Message | General Type | Trouble Id | Device Type | Address | Serial number | Location | Inactive | Cleared | Acknowledge
4/10/2006 4:14:09 PM | Relay config = factory defaults | Trouble | 30 | LaserSCANNER Display | 5.003.20 | 106195 | VLS Display
4/10/2006 4:14:08 PM | Relays not found | Trouble | 16 | VESDA LaserSCANNER FA | 5.020 | 71403 | MCG
4/10/2006 4:14:08 PM | No communication from ancillary devic | Trouble | 24 | VESDA LaserSCANNER FA | 5.020 | 71403 | MCG
4/10/2006 4:14:08 PM | LaserSCANNER option misconfigured | Trouble | 28 | VESDA LaserSCANNER FA | 5.020 | 71403 | MCG
4/10/2006 4:14:03 PM | Filter approaching capacity | Trouble | 11 | VESDA LaserSCANNER | 5.003 | 4 | Opera House
4/10/2006 4:14:03 PM | No communication from ancillary devic | Trouble | 24 | VESDA LaserSCANNER | 5.003 | 4 | Opera House
4/10/2006 4:13:29 PM | Comms fault on VESDAnet Port A | Trouble | 2 | VESDA Display | 5.007.20 | 92994 | Reception
4/10/2006 4:13:15 PM | LaserSCANNER option misconfigured | Trouble | 28 | VESDA Display | 5.020.21 | 88024 | Harbour Bridge
4/10/2006 4:14:09 PM
LaserSCANNER Display (5.003.20)
VLS Display - Relay config = factory defaults
Ready
designer : Designer
Connected

Figure 4-8: Active Event List

Specific help is available for events by selecting the event and then pressing **F1**. In the case of Troubles this will indicate actions that can be taken to alleviate the condition.

Acknowledging Events

To acknowledge events, select them and then click the Acknowledge toolbar button (the one with the tick). Multiple events can be selected and acknowledged in the one operation.

Resetting a Device

Select the Reset button, located in the status bar, or select an event(s) on the Active Event List and click on the toolbar Reset button. This will reset the device associated with the event and clear out all its active events. Any current events will be regenerated as they are encountered so that if the condition that caused the event has not been rectified, that event will reappear.

Silence

Select the Silence button, located in the notification bar, to temporarily silence the outputs of the device associated with the event. Pressing the button again will un-silence the outputs.

4.2 Monitored Conditions

VSM4 monitors the fire detection system for a range of alarms and troubles which are broken into more specific categories to provide greater control and flexibility in reporting and responding to them. The more detailed categories (in priority order) are:

Condition	Description
Fire 1	An alarm indicating a significant fire event.
Fire 2	An alarm indicating the presence of a fire.
Non-fire Alarm	A condition that indicates an alarm due to another cause such as a Tornado.
Action	There are indications of a fire that warrant investigation but not sufficient to generate an alarm.
Alert	The fire indication is higher than the background level.
Supervisory	An urgent trouble that compromises the fire system such as freezing of water in a sprinkler system.
Trouble	There is a fault with a component of the system.
Disabled	Indicates that a device has been disabled or that a disabled device is generating alarms or troubles.
Mismatched Devices	The monitored system differs from what is expected. This can appear as: • A device appears where none was expected. • An expected device is missing. • A device of a different type appears in place of another. • A configured network connection has dropped out.
None	This is just the absence of any condition which indicates that the system is running as expected.

Table 4-1: Monitored Conditions

As monitored conditions appear or disappear they are added to and removed from the Active Event List, which drives the key monitoring views. It causes the state of zones in the floor plans to change and updates the icons on the floor plan tree. Emails may also be sent to User groups.

4.2.1 Condition Priority

When multiple conditions are currently active then a priority scheme is used to focus the operator's attention to the most critical ones.

The Active Event List prioritizes events in the following order:

1. **Acknowledged State** – fresh events that the operator has not yet reviewed are given higher priority than ones that have been acknowledged. (The acknowledge behavior and policies are described below).
2. **Event Type** – the category of the condition is prioritized as shown above.
3. **Timestamp** – recent events are given prominence over older events.

The Floor Plan zones show the condition of the associated detector. Again it is possible that several conditions may be simultaneously active. In this case the category of the event becomes more important than whether it has been acknowledged by the operator and so priority rules have the following order:

1. Event Type
2. Acknowledged State
3. Timestamp

4.2.2 Display Highest Priority Condition

When the highest priority event has changed, the user is notified in several ways:

- the status bar at the bottom of the application window updates.
- the event is annunciated by Text-to-Speech (if installed).
- If the event type is Alarm or Pre-Alarm, the Floor Plan automatically switches to the appropriate page and the associated area on the page relating to the responsible device updates.
- if responses have been configured, the Browser will display the corresponding document.

4.3 Acknowledging an Incident

An operator may not immediately notice intermittent events that come and go. The way VSM4 responds depends on the acknowledge and latching behavior that was set up by the Designer. Acknowledgement means that events need to be explicitly acknowledged by the operator before they can be removed from the list of Active Events. Latching means that events will not be removed from the list until the device is reset.

The three state attributes; Acknowledged, Inactive and Cleared, show the state of an event.

- **Acknowledged** indicates that an event has been acknowledged by the operator.
- **Inactive** indicates that the device has stopped reporting the event condition. This may happen for an intermittent trouble. The presence of an event in this state in the list indicates that either the operator has not yet acknowledged this event or that event latching is enabled and the device has not yet been reset.
- **Cleared** indicates that the event condition has gone away and that the device has been reset but that the VSM4 operator has not yet acknowledged this event. Once acknowledged it will be cleared from the list.

4.3.1 Acknowledging an Event

An event should be Acknowledged to indicate that it has been seen by the operator. This will cause it to stop flashing.

Events can be acknowledged from several views:

- If the event is being viewed on the Status Bar then the Acknowledge button on the Status Bar should be used.
- If the event is being viewed on the Active Event List then it should be selected and then the Acknowledge button on the toolbar should be clicked. Multiple events can be selected and acknowledged together using the Active Event List.

4.3.2 Acknowledging Related Events

As smoke increases, a detector will typically generate Alert, Action and Fire events. Each of these stays in the Active Event List so that the operator can readily see the relative time at which they occurred. When one of these events is acknowledged then all older, related events (for this detector) are implicitly acknowledged.

Once an event has been acknowledged then it will drop in priority compared with any unacknowledged events. As a result acknowledging an event on the Status Bar can cause another unacknowledged event to take its place so that the Status Bar will continue flashing, but the event details will differ.

4.4 Event Management Options

The Event Management Tab of the Options dialog (Figure 4-9) is used to select the type of events that will remain in the Active Event List until they are reset or acknowledged.

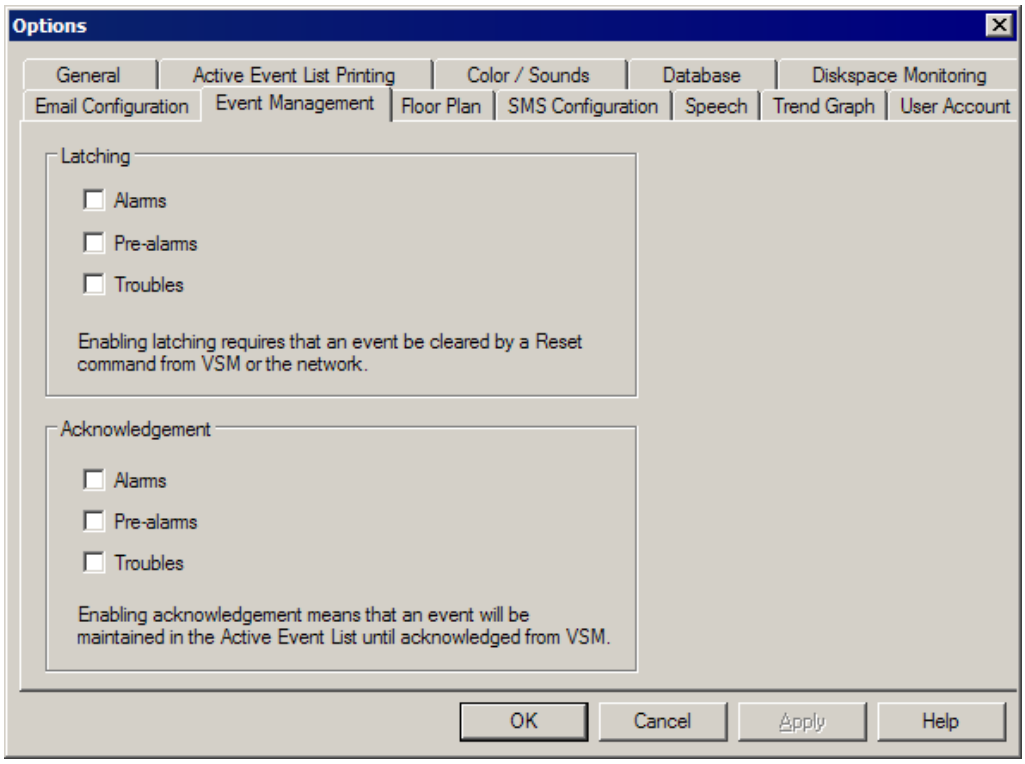


Figure 4-9: View > Options > Event Management

- **Latching -** The settings for specifying which events will be retained in the Active Event List until the device that generated the event is reset.
  - Alarms - If checked, alarm events will remain in the Active Event List until they are reset.
  - Pre-Alarms - If checked, pre-alarm events will remain in the Active Event List until they are reset.
  - Trouble - If checked, trouble events will remain in the Active Event List until they are reset.
- **Acknowledgement -** The settings for specifying which events require acknowledgement.
  - Alarms - If checked, alarm events will remain in the Active Event List until they are acknowledged.
  - Pre-Alarms - If checked, pre-alarm events will remain in the Active Event List until they are acknowledged.
  - Trouble - If checked, trouble events will remain in the Active Event List until they are acknowledged.

4.5 Device Status

VSM4 routinely monitors a range of detector status such as the current smoke level (or temperature), air flow, filter status, etc. The availability of these properties depend on the feature set of the actual detector.

The device status can be viewed in several ways. If you want to drill into a specific device then double click on that device in the floor plan (or floor plan tree) and a status window will be displayed. However, if you would like to compare several properties of several detectors then the best way is to view them in a grid. Alternatively, if you are interested in comparing the time variation of the smoke (or temperature) measurements of several detectors then use the graph.

4.5.1 Status View

The current status of a live device can be viewed in the Status view. The Status view may appear in the detail pane on a Device view when the device is selected on the tree. Alternately, a floating Status view can be created by selecting **View > Status**.

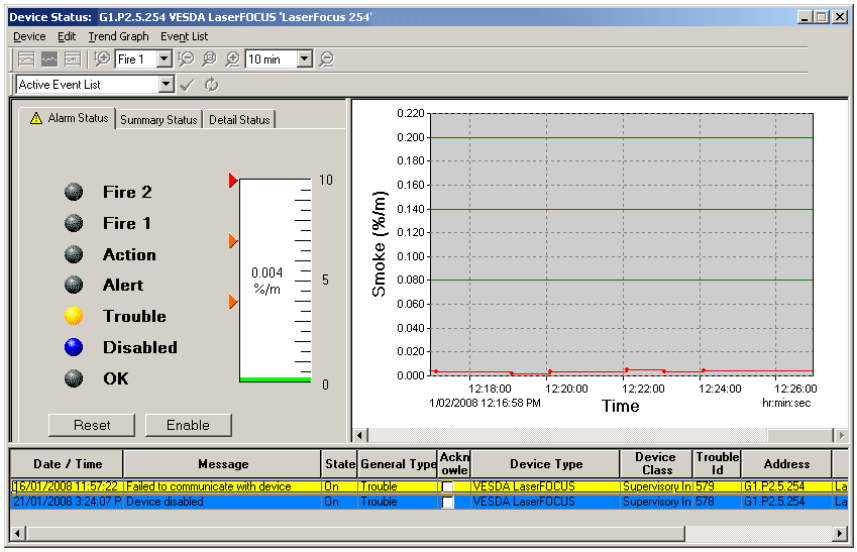


Figure 4-10: Status View (floating)

The status view combines a trend graph, an Active Event List and status pages that are all restricted to the selected device and any associated devices.

The Trend graph and Active Event list sub-views behave identically to the standard views (see Section 7.9 and 7.2) and have the same menus and toolbar buttons. The graph shows the variation in the measured value with time, so that trends can be readily observed. The Active Event List allows troubles and alarms directly associated with the device to be readily observed and acknowledged.

The Trend Graph tab of the Options dialog (Figure 4-11) sets the cache size for devices which determines the history that is immediately available to the Status View when the device is selected and the Status View shown. Increasing cache size will consume more RAM and so an estimate of this is shown on the dialog.

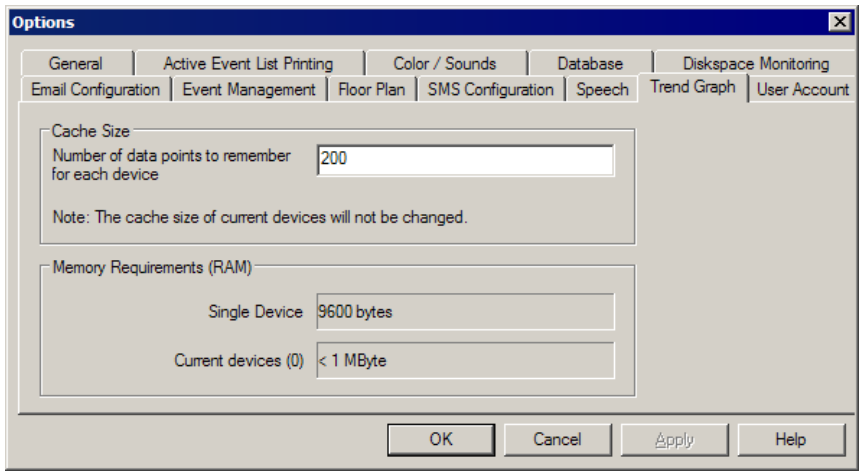


Figure 4-11: View > Options > Trend Graph

Trend Graph Settings

- **Cache Size -** Enter the number of data points to remember for each device. The cache size of current devices will not be changed. Disconnect and reconnect to the device to view the change to the cache size.
- **Memory Requirements (RAM) -** The memory requirement calculations for the cache size are displayed. These fields are not editable.

Status Pages

The Status pages provide the following information:

- **Alarm status -** This tab applies only for detectors and contains primary information in graphic format, including a traffic light indicator which shows the event level, and a bar graph showing the current smoke level from a detector (or temperature for a heat detector).
- **Summary status -** This tab contains primary information in text format, including alarm status, smoke level, current airflow and filter status.
- **Detail status -** This tab contains detailed status information in tabular format.
- **Associations -** This tab contains a list of devices that are associated with the original device, such as reference detectors or display units.

Viewing Detector Status in a Grid

1. Open a Monitoring Structure by clicking on the Floor Plan and then selecting **View > Monitor Browser**. This provides a network-centric view of the system.
2. Select the relevant network or loop and the detectors will be shown in the grid on the right side.
3. Select **Device View > Hide Empty Rows** to remove all unused address rows from the grid.
4. Click on the combo-box in the toolbar and select the Status style which will show a set of live status settings. The Status style has been setup for VESDAnet. If it doesn't currently exist for the loop you are interested in then select **Device View > Grid Style Manager** and create your own style. If the Status style exists but doesn't have all the properties that you wish then create your own style based on the default Status style.
   Notes
   - You can not edit the default system styles but you can add additional styles as needed.
   - Air Flow and Filter status settings will not be updated on a grid due to VESDAnet limitations, so don't include them on your style.

There will be times when you will want to compare detectors from different loops. To do this:

1. Select a node in the tree which contains all the relevant detectors.
2. Select **Device View > All Devices** to cause all descendent devices to appear on the right side with addresses that are relevant to the selected tree node.
3. Select a status style, or create your own style.

With this approach it would be possible to view the status of all devices in the entire system in the one table.

Remember you can sort on any of the columns, including Device Type to group the devices.

4.5.2 Trend Graphs

The time variation of the detector's measured values can be shown on the Trend graph. As the name suggests this allows trends in the readings to be visually separated from noise. For pre-alarms this could distinguish between a slow buildup of smoke causing an Alert threshold to be tripped or a threshold that has been set too low and is in the signal noise. The Trend graph allows multiple devices to be plotted so that their readings can be visually compared.

Open the Trend Graph

Select an icon or region that represents a detector and then invoke **View > Trend Graph** from its context menu to graph the detector. The operator is prompted with a filter window (see below) where they can choose to plot historical and/or live measurements.

- **Live -** Displays readings as the data is received.
- **Historical -** Displays readings from the database or the device's event log. The plotted events can be restricted to a specific time and date range.

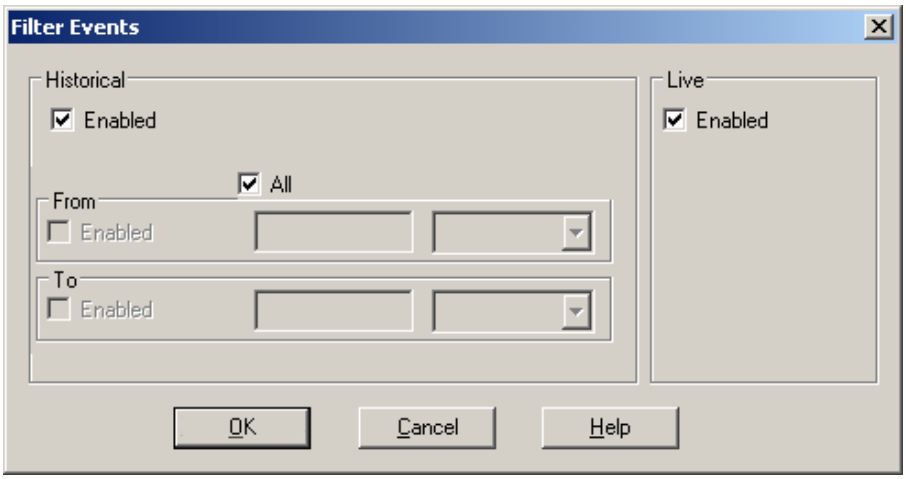


Figure 4-12: Trend Graph Filter Dialog

After making a selection, a new graph view is opened, unless one is already open for the current connection. If a trend graph view is already open then the selected detector is added to it. Additional devices can be added by repeating the above steps or by drag and dropping them onto the graph. For example, multiple devices can be selected in a grid and dragged and dropped onto a graph.

Note: Graphs will currently only accept devices sharing the same connection since the graph uses the network time (associated with the connection) for its time axis.

Trend Graph Elements

A trend graph will contain multiple sub-graphs as shown below, when devices that measure different quantities are plotted against each other. Each sub-graph is associated with a specific quantity. For example, in the graph below, the top sub-graph shows outputs from two devices in raw units and the lower sub-graph shows smoke measurements. All sub-graphs share the same time scale and so

scroll together. The legend appears to the right of each sub-graph. It lists the devices that are plotted and allows commands on these devices to be invoked by using a context menu.

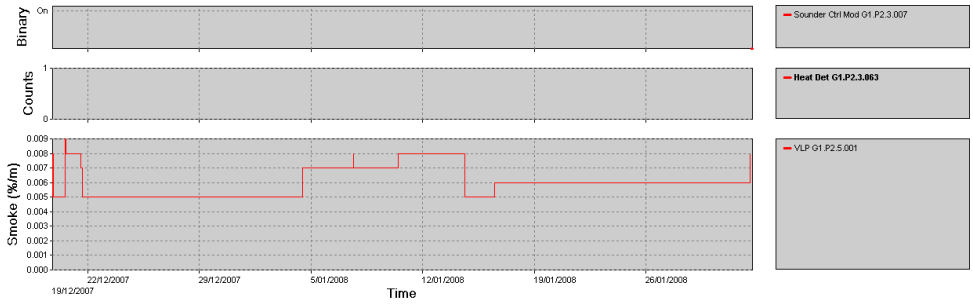


Figure 4-13: Trend Graph

Legend

The legend defines the color for each plotted device and identifies the detector by acronym and address. Detectors with multiple inputs such as the VLS show a line for each input.

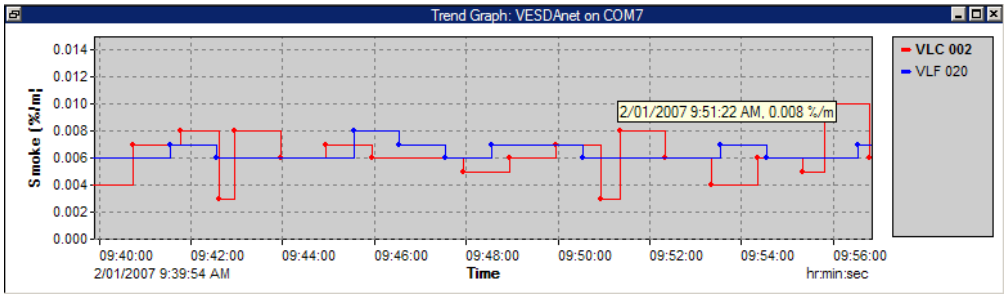


Figure 4-14: Trend Graph View with Legend

When multiple devices are plotted one is defined as the 'current' device and is shown bolded in the legend. The current device defines the threshold levels which are shown on the graph and which are used to define the Fire1 and Fire2 vertical scales.

Hiding/Showing Device

Right-clicking on a device entry in the legend will bring up a context menu which allows devices to be hidden or shown on the graph. Hidden devices are shown as greyed-out entries on the legend.

Removing Device

Right-click on the device entry in the legend in the legend and select **Delete** from the context menu. Alternatively, left-click on the device entry in the legend and select **Delete**.

Device Commands and Views

The context menu provides access to commands and views that are relevant to the device.

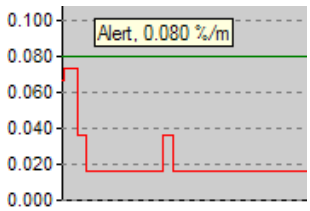


Figure 4-15: Trend Graph Threshold Level

Display

Thresholds

Green horizontal lines indicate the thresholds for the currently selected device (e.g. Fire 1, Fire 2). To identify a threshold line and see its exact value, position the mouse pointer over it and read the tooltip, as shown below.

Some of the more sophisticated detectors have separate threshold banks for day and night operation and will automatically swap between these banks. The operator can choose to show the Day, Night or Current thresholds on the graph by clicking on the relevant button on the graph toolbar.

Data Points

Points where the measured reading changed are shown as round dots if the graph is zoomed in sufficiently. As the graph is zoomed out the dots disappear and only the line remains, as shown above. Points where readings ceased or restarted, due for example to the loss of power, are shown as breaks in the graph.

Tool Tips

Show data values by positioning the mouse pointer over the rounded dots located at value change points along the line to view the exact date, time and smoke value at that point.

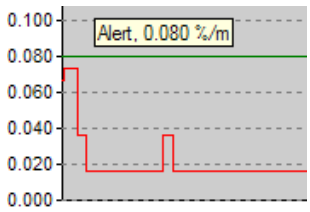


Figure 4-16: Tooltip showing the name and value of the threshold level

Trend Graph Navigation

The graph allows the user to zoom and pan through the data to locate and view relevant data.

Zooming

Toolbar buttons and menu commands are provided for the zoom as detailed below. The zoom can also be specified by clicking on a graph and dragging out a rectangular region of interest. The graph will scale to this region. If the shift key is held down while dragging out the region then only the time range will be affected; the vertical range will remain the same.

Panning

The horizontal and vertical scrollbars are used to pan the view. The vertical scroll bar will not be shown if all the data points are already within the vertical range of the graph.

Live Setting

The Trend Graph display will track live data if the graph is scrolled to include the current time by scrolling the horizontal scroll bar to the extreme right.

When this is done the right arrow at the end of the scroll bar is disabled. If the scroll bar is moved to the left, or the user zooms in on data at an earlier time, then the graph display will stay locked on the specified time range and the scroll bar will move to the left as the displayed time falls further behind the current time.

Toolbar and Menu

The Trend Graph Toolbar is shown below:

Figure 4-17: Trend Graph Toolbar

- The first three buttons act as radio buttons to specify the thresholds. They specify the day, night and current detector thresholds, respectively.
- The vertical magnification buttons specify the vertical zoom in, special zoom and zoom out.
- The special zoom dropdown lets the range be set to standard pre-defined values as shown below.

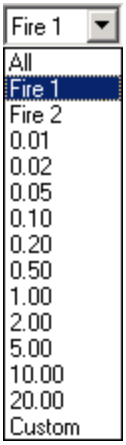


Figure 4-18: Setting the Vertical Zoom

- The Show All button will set the horizontal and vertical ranges to cover all the data points.
- The horizontal magnification buttons specify the horizontal zoom in, special zoom and zoom out.
- The Menu lists the functions of the toolbar except for the special zoom options.

4.6 Connection Status

A summary of the status of all connections associated with the current monitoring site can be accessed by selecting **Connection > View Used Connections** from the menu system.

The table (Figure 4-19) shows the state of all connections color coded according to their state. Red indicates broken connections and green indicates a normal connection. Where a broken connection exists, the number of retries is also tabulated.

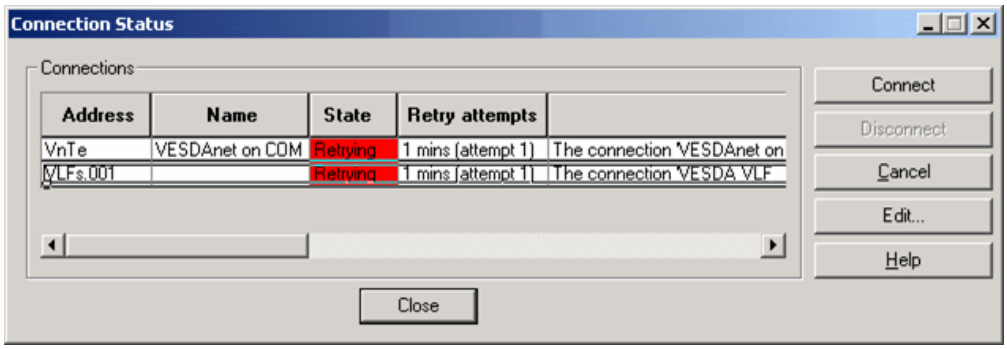


Figure 4-19: Connection Status

Operations

The buttons provide operations that apply to the connection that is currently selected within the table.

- The **Connect** button will attempt to immediately reconnect broken connections (without waiting for the retry time).
- The **Disconnect** button will break the connection.
- The **Cancel** button will cancel an attempt to open a connection.
- The **Edit** button will bring up the connection tab to allow another connection file to be used or allow retry times or predefined PINs to be edited.

5 Investigation

VSM4 provides tools to review current and past detector performance and state so that past incidents can be investigated. Event logs are kept of user actions and state changes throughout the system. Changes in measured detector values, such as smoke, are logged. This data can be viewed in tabular form in Event Logs and plotted in Trend Graphs.

5.1 Investigation Tools

VSM4 provides a range of tools to enable administrators to review system operation, fine-tune system settings or to troubleshoot equipment faults.

These tools include:

- **The Event Log -** Logs of user actions and state changes are maintained within Xtralis VESDA detectors, and can be inspected to investigate incidents.
- **The System Log -** The System log records user activity within VSM4. It is often used in conjunction with the Event Log to associate operators with incidents.
- **Trend Graphs -** The Trend Graph displays a line graph of the smoke level for the selected detector(s) over the nominated period of time, and was described in the previous chapter (section 4.5.2).
- **Comparison / Merge Tool -** This view allows network and device configurations to be compared. In particular, it supports system auditing by highlighting any configuration changes since the installed and commissioned system.

5.1.1 Event Log

Event Logs are maintained within Xtralis VESDA detectors, and record state changes and user actions. VSM4 should be setup by the Designer to integrate these logs into a database (refer to Chapter 3).

The Event Log View displays these historical events. It can be used by an administrator to verify correct system operation, fine-tune system settings or to troubleshoot equipment faults. Event data may be loaded from a file, retrieved from a detector or obtained from a database.

Open Event Log View

Select **View > View Database Events** or click on the Event Log view button on the main toolbar to open a view of the events.

Note: The Event Log toolbar button defaults to the database events when available, otherwise it will source the event data directly from the device.

Before the Event Log is opened, the Filter Events dialog is displayed. For example, Figure 5-1 shows the filter for the database.

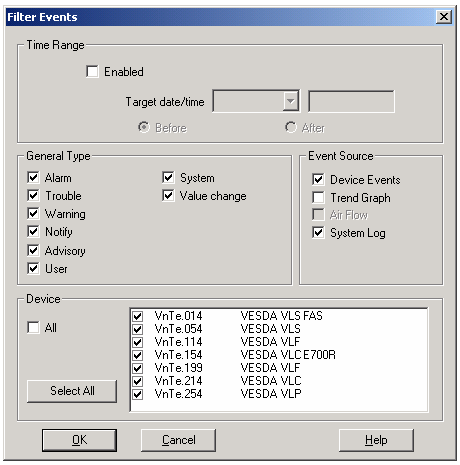


Figure 5-1: Filter Events

The panels on the filter allow the user to define:

- When the events occurred (i.e. the relevant time range). A starting date/time or a finishing date/time can be defined.
- The type of events that are relevant.
- The source of the events, e.g. device events, trend data or system events. The system events show who is logged onto VSM4 and so can be used to associate an operator with an action.
- Where they occurred, i.e. which devices to collect events for.

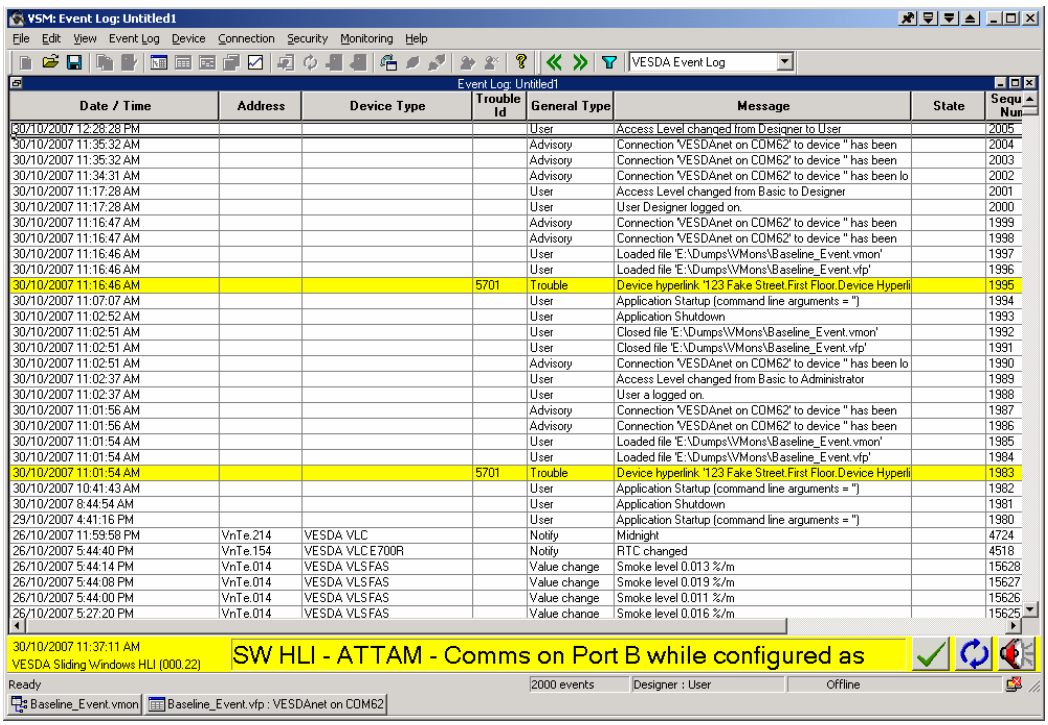

VSM: Event Log: Untitled1
File Edit View Event Log Device Connection Security Monitoring Help
VESDA Event Log
Event Log: Untitled1
Date / Time | Address | Device Type | Trouble Id | General Type | Message | State | Sequ Num
30/10/2007 12:28:28 PM User Access Level changed from Designer to User 2005
30/10/2007 11:35:32 AM Advisory Connection 'VESDAnet on COM62' to device '' has been 2004
30/10/2007 11:35:32 AM Advisory Connection 'VESDAnet on COM62' to device '' has been 2003
30/10/2007 11:34:31 AM Advisory Connection 'VESDAnet on COM62' to device '' has been lo 2002
30/10/2007 11:17:28 AM User Access Level changed from Basic to Designer 2001
30/10/2007 11:17:28 AM User User Designer logged on. 2000
30/10/2007 11:16:47 AM Advisory Connection 'VESDAnet on COM62' to device '' has been 1999
30/10/2007 11:16:47 AM Advisory Connection 'VESDAnet on COM62' to device '' has been 1998
30/10/2007 11:16:46 AM User Loaded file 'E:\Dumps\VMons\Baseline_Event.vmon' 1997
30/10/2007 11:16:46 AM User Loaded file 'E:\Dumps\VMons\Baseline_Event.vfp' 1996
30/10/2007 11:16:46 AM 5701 Trouble Device hyperlink '123 Fake Street.First Floor.Device Hyperli 1995
30/10/2007 11:07:07 AM User Application Startup (command line arguments = '') 1994
30/10/2007 11:02:52 AM User Application Shutdown 1993
30/10/2007 11:02:51 AM User Closed file 'E:\Dumps\VMons\Baseline_Event.vmon' 1992
30/10/2007 11:02:51 AM User Closed file 'E:\Dumps\VMons\Baseline_Event.vfp' 1991
30/10/2007 11:02:51 AM Advisory Connection 'VESDAnet on COM62' to device '' has been lo 1990
30/10/2007 11:02:37 AM User Access Level changed from Basic to Administrator 1989
30/10/2007 11:02:37 AM User User a logged on. 1988
30/10/2007 11:01:56 AM Advisory Connection 'VESDAnet on COM62' to device '' has been 1987
30/10/2007 11:01:56 AM Advisory Connection 'VESDAnet on COM62' to device '' has been 1986
30/10/2007 11:01:54 AM User Loaded file 'E:\Dumps\VMons\Baseline_Event.vmon' 1985
30/10/2007 11:01:54 AM User Loaded file 'E:\Dumps\VMons\Baseline_Event.vfp' 1984
30/10/2007 11:01:54 AM 5701 Trouble Device hyperlink '123 Fake Street.First Floor.Device Hyperli 1983
30/10/2007 10:41:43 AM User Application Startup (command line arguments = '') 1982
30/10/2007 8:44:54 AM User Application Shutdown 1981
29/10/2007 4:41:16 PM User Application Startup (command line arguments = '') 1980
26/10/2007 11:59:58 PM VnTe.214 VESDA VLC Notify Midnight 4724
26/10/2007 5:44:40 PM VnTe.154 VESDA VLC E700R Notify RTC changed 4518
26/10/2007 5:44:14 PM VnTe.014 VESDA VLS FAS Value change Smoke level 0.013 %/m 15628
26/10/2007 5:44:08 PM VnTe.014 VESDA VLS FAS Value change Smoke level 0.019 %/m 15627
26/10/2007 5:44:00 PM VnTe.014 VESDA VLS FAS Value change Smoke level 0.011 %/m 15626
26/10/2007 5:27:20 PM VnTe.014 VESDA VLS FAS Value change Smoke level 0.016 %/m 15625
30/10/2007 11:37:11 AM
VESDA Sliding Windows HLI (000.22)
SW HLI - ATTAM - Comms on Port B while configured as
Ready
2000 events
Designer : User
Offline
Baseline_Event.vmon
Baseline_Event.vfp : VESDAnet on COM62

Figure 5-2: Event Log for a VLS

Event data can be trended using the Trend Graph (select **View > Trend Graph**). This option will only be available if there are points available for plotting.

Event Retrieval

Once the data has been retrieved the number of events is shown in a panel below the status bar. Page forward/backward buttons are provided on the toolbar to request further events going forwards from the most recent or backwards from the oldest of the displayed events. The maximum number of viewed events is 20,000. Once this limit has been reached paging forwards to further events will cull the oldest events. Similarly paging backward will cull the earliest events.

The filter toolbar button allows the displayed data to be further filtered. It brings up the Filter Events dialog shown above. If the filter conditions are made more restrictive, then the filtering is done in RAM and is fast. If the filter conditions are relaxed beyond the conditions associated with the original database retrieve then the data will be fetched again from the database which is slower.

The Event Log menu provides access to the Grid Style Manager as well as these event retrieval and filtering commands.

Event Log Display Controls

The Event Log table style can be changed to one of the pre-defined ones by using the table style selector on the toolbar. Additional table styles can be created using the Grid Style Manager (section 7.2.6):

- **Sorting -** The Event Log table can be sorted by column. This is done by clicking on the heading of the desired column. This will sort in ascending order. Clicking again will toggle it to sort in descending order.

Saving / Loading Event Logs

Event logs can be saved in binary file (i.e. in .vevt format) by selecting **File > Save As**. These files can be reloaded into VSM4 using **File > Open**, and are language neutral.

Exporting

Event logs can be exported to a text file with the data in the columns, tab separated. Such files can be loaded into spreadsheets for further analysis.

Note: VSM4 is unable to load these files.

The contents of the Event Log table can be copied to the Windows clipboard. To achieve this, left-click and drag over a range of events in the list, then press CTRL+C. The copied data is formatted using tab delimiters in-between columns. The column headings are automatically included in the exported data.

Printing Event Data

The **File > Print** (and Print Preview) commands allow an event log to be printed out. Where the printed table exceeds a single page the column headings are repeated on each page.

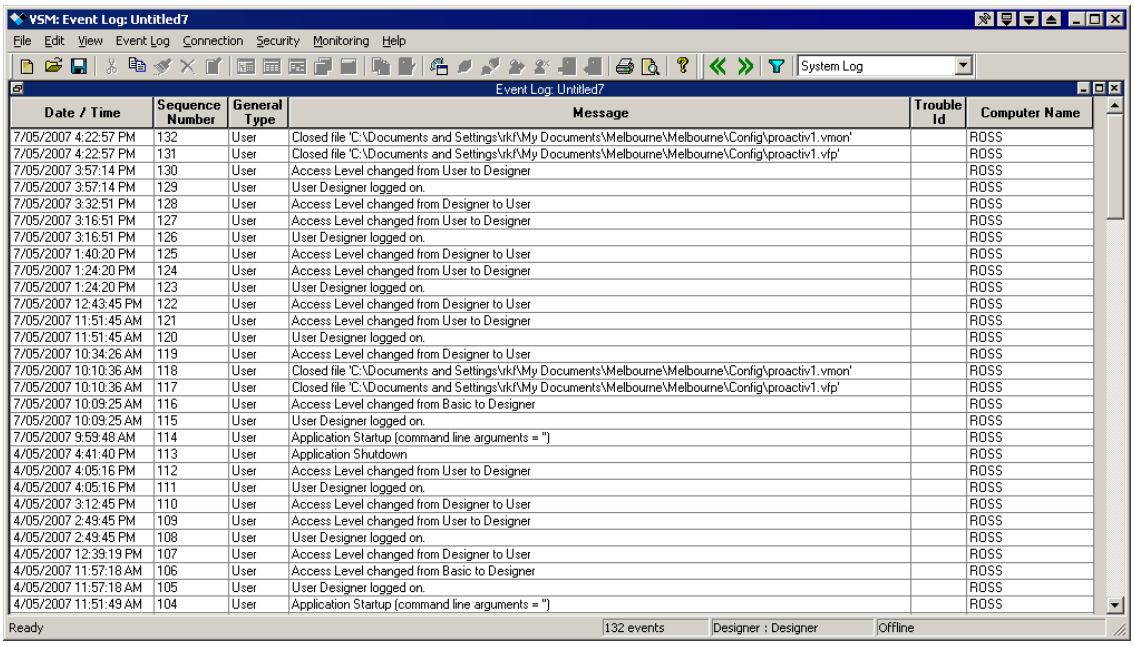
Plotting Event Data

Event data can be trended using the Trend Graph (select **View > Trend Graph**).

5.1.2 System Log

The System Log is an event log that displays user and system events. For example, the system log records whenever the application starts or stops, access level changes and when Monitoring View and Floor Plan files are opened. This allows administrators to track user activity by user us. The System Log can be viewed in conjunction with device events by checking 'System Log' as a source in the database filter. Alternatively, the system log can be viewed by itself using **Monitoring > View System Log**. The filter that is then used is simpler than that used for device events (as seen below) since it has only one source and no devices.

An example System Log View is shown in Figure 5-3 (below).



Date / Time	Sequence Number	General Type	Message	Trouble Id	Computer Name
7/05/2007 4:22:57 PM	132	User	Closed file 'C:\Documents and Settings\rkf\My Documents\Melbourne\Melbourne\Config\proactiv1.vmon'		ROSS
7/05/2007 4:22:57 PM	131	User	Closed file 'C:\Documents and Settings\rkf\My Documents\Melbourne\Melbourne\Config\proactiv1.vfp'		ROSS
7/05/2007 3:57:14 PM	130	User	Access Level changed from User to Designer		ROSS
7/05/2007 3:57:14 PM	129	User	User Designer logged on.		ROSS
7/05/2007 3:32:51 PM	128	User	Access Level changed from Designer to User		ROSS
7/05/2007 3:16:51 PM	127	User	Access Level changed from User to Designer		ROSS
7/05/2007 3:16:51 PM	126	User	User Designer logged on.		ROSS
7/05/2007 1:40:20 PM	125	User	Access Level changed from Designer to User		ROSS
7/05/2007 1:24:20 PM	124	User	Access Level changed from User to Designer		ROSS
7/05/2007 1:24:20 PM	123	User	User Designer logged on.		ROSS
7/05/2007 12:43:45 PM	122	User	Access Level changed from Designer to User		ROSS
7/05/2007 11:51:45 AM	121	User	Access Level changed from User to Designer		ROSS
7/05/2007 11:51:45 AM	120	User	User Designer logged on.		ROSS
7/05/2007 10:34:26 AM	119	User	Access Level changed from Designer to User		ROSS
7/05/2007 10:10:36 AM	118	User	Closed file 'C:\Documents and Settings\rkf\My Documents\Melbourne\Melbourne\Config\proactiv1.vmon'		ROSS
7/05/2007 10:10:36 AM	117	User	Closed file 'C:\Documents and Settings\rkf\My Documents\Melbourne\Melbourne\Config\proactiv1.vfp'		ROSS
7/05/2007 10:09:25 AM	116	User	Access Level changed from Basic to Designer		ROSS
7/05/2007 10:09:25 AM	115	User	User Designer logged on.		ROSS
7/05/2007 9:59:48 AM	114	User	Application Startup (command line arguments = '')		ROSS
4/05/2007 4:41:40 PM	113	User	Application Shutdown		ROSS
4/05/2007 4:05:16 PM	112	User	Access Level changed from User to Designer		ROSS
4/05/2007 4:05:16 PM	111	User	User Designer logged on.		ROSS
4/05/2007 3:12:45 PM	110	User	Access Level changed from Designer to User		ROSS
4/05/2007 2:49:45 PM	109	User	Access Level changed from User to Designer		ROSS
4/05/2007 2:49:45 PM	108	User	User Designer logged on.		ROSS
4/05/2007 12:39:19 PM	107	User	Access Level changed from Designer to User		ROSS
4/05/2007 11:57:18 AM	106	User	Access Level changed from Basic to Designer		ROSS
4/05/2007 11:57:18 AM	105	User	User Designer logged on.		ROSS
4/05/2007 11:51:49 AM	104	User	Application Startup (command line arguments = '')		ROSS

Figure 5-3: System Log View

Refer to section 3.4.2 for information on enabling the System Log.

5.1.3 Comparison / Merge Tool

When reviewing a system, the current configuration can be compared to an earlier working version, such as when the system was installed and commissioned. The Comparison tool allows comparisons between equivalent items. The devices being compared may be live or offline, they may be simple devices or networks, but they must be of the same type. Using this tool configuration differences can be readily identified, and if needed, undone.

To launch the Comparison tool select the device of interest and then click on the **Compare/Merge** toolbar button. The cursor will then change.

- The cursor will appear as the invalid target icon until it is moved over a valid reference device.
- If the starting device is write-protected (i.e. the operator is not logged on at Admin level) then the cursor will change to a magnifying glass, indicating that a comparison will be made.
- If the starting device can be edited then the cursor will be an eye-dropper to indicate that settings will be pulled from the reference device and merged with the initial device.

Clicking on a valid reference device will launch the Comparison / Merge tool.

Compare

The Compare Configurations view shows a device hierarchy on the left and a list of settings on the right corresponding to the node selected in the tree.

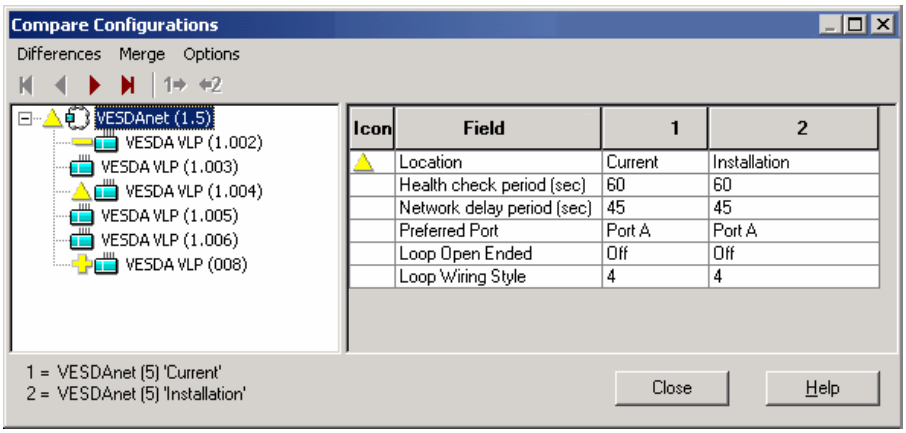


Figure 5-4: Comparison View of two VESDAnets

The columns in the table labeled 1 and 2 refer to the original device and the reference device. The type, address and location of these two devices are shown as a legend at the lower left of the dialog.

The icons next to the tree nodes and settings have the following meaning:

Icon	Description
	This node or setting has not changed.
	This node did not exist in the original device and has been added in the reference device.
	This node did exist in the original device and has been removed in the reference device.
	This node or setting has changed.
	This setting has changed but may not be directly edited in the merge tool. (Applies mainly to complex settings like relay masks and interlocking).
	This device has not changed but one of its children has.

Navigation

The toolbar contains a navigation panel and a merge panel (discussed below). The navigation controls have the meaning tabulated below and also have equivalent menus commands under the Differences menu.

Button	Description
	Step to first difference
	Step to last difference
	Step to previous difference
	Step to next difference

Table 5-1: Comparison / Merge Tool Navigation Buttons

The icons are disabled when not valid. For example, when the first different device is selected then ‘Step to first difference’ and ‘Step to previous difference’ commands (and toolbar buttons) will be disabled.

Show Only Differences

Select **Options > Show Differences Only** to hide all non-differences so that the differences are easier to see. The default mode shows all devices and properties.

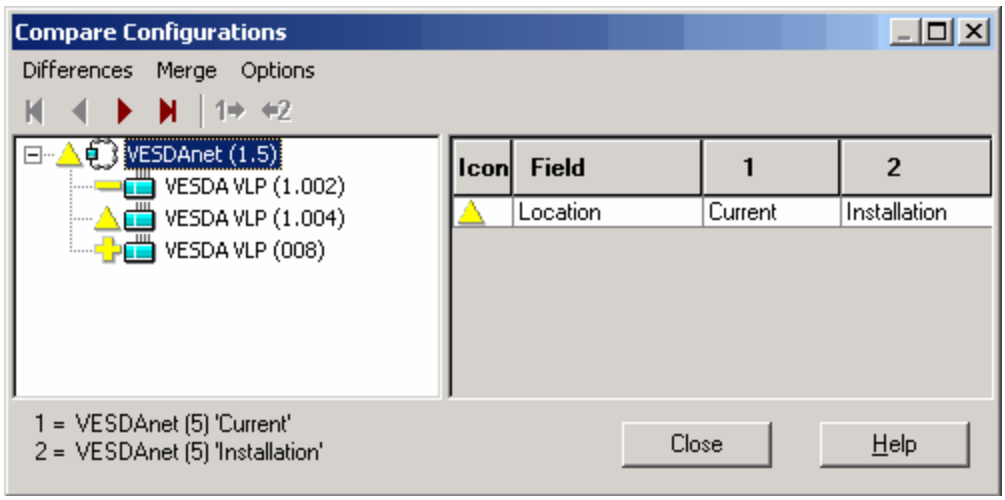


Figure 5-5: Merge two VESDAnets - show only differences

Merge

Running through the same example as above but logged on at Admin level brings up the Merge tool.

The table now contains an extra column, Target After Merge, that shows the results of the merge. By default the merge will leave the target (i.e. the original device) unchanged.

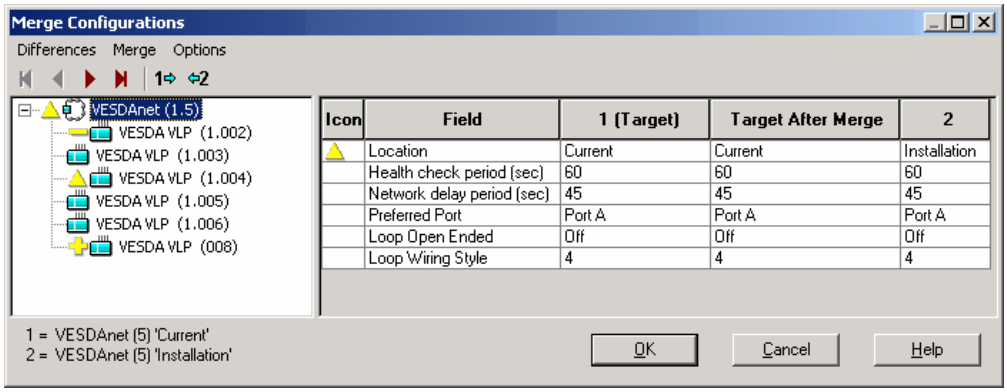

Merge Configurations
Differences Merge Options
VESDAnet (1.5)
VESDA VLP (1.002)
VESDA VLP (1.003)
VESDA VLP (1.004)
VESDA VLP (1.005)
VESDA VLP (1.006)
VESDA VLP (008)
Icon Field 1 (Target) Target After Merge 2
Location Current Current Installation
Health check period (sec) 60 60 60
Network delay period (sec) 45 45 45
Preferred Port Port A Port A Port A
Loop Open Ended Off Off Off
Loop Wiring Style 4 4 4
1 = VESDAnet (5) 'Current'
2 = VESDAnet (5) 'Installation'
OK
Cancel
Help

Figure 5-6: Merging two VESDAnets (Merged Device)

Button	Description
1⇨	Merge 1 - takes the values of the target (i.e. device 1) and places them in the merged output.
⇦2	Merge 2 - takes the values from the reference device (i.e. device 2) and place them in the merged output.

The Merge menu and toolbar buttons are now enabled.

Merges affect the current level and everything below it. For example, to accept all the reference loop settings, the top node in the tree would be selected and the **Merge 2** button pressed. To keep just the original location setting on the VLP at address 4, then this device would be selected in the tree and just this setting selected in the table, as shown below, and the **Merge 1** button pressed.

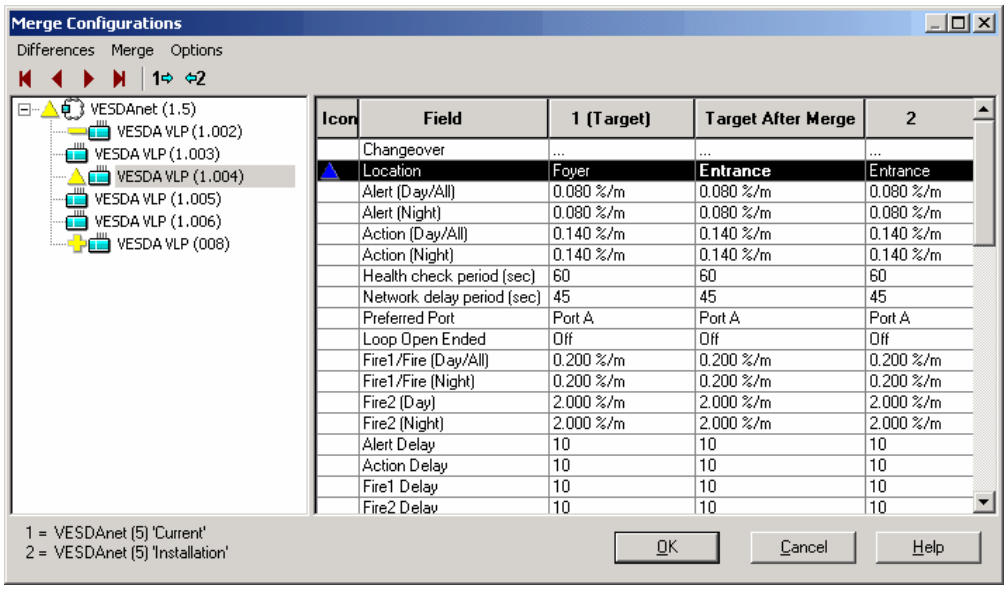

Merge Configurations
Differences Merge Options
1⇨ ⇦2
VESDAnet (1.5)
VESDA VLP (1.002)
VESDA VLP (1.003)
VESDA VLP (1.004)
VESDA VLP (1.005)
VESDA VLP (1.006)
VESDA VLP (008)
Icon
Field
1 (Target)
Target After Merge
2
Changeover ... ...
Location Foyer Entrance Entrance
Alert (Day/All) 0.080 %/m 0.080 %/m 0.080 %/m
Alert (Night) 0.080 %/m 0.080 %/m 0.080 %/m
Action (Day/All) 0.140 %/m 0.140 %/m 0.140 %/m
Action (Night) 0.140 %/m 0.140 %/m 0.140 %/m
Health check period (sec) 60 60 60
Network delay period (sec) 45 45 45
Preferred Port Port A Port A Port A
Loop Open Ended Off Off Off
Fire1/Fire (Day/All) 0.200 %/m 0.200 %/m 0.200 %/m
Fire1/Fire (Night) 0.200 %/m 0.200 %/m 0.200 %/m
Fire2 (Day) 2.000 %/m 2.000 %/m 2.000 %/m
Fire2 (Night) 2.000 %/m 2.000 %/m 2.000 %/m
Alert Delay 10 10 10
Action Delay 10 10 10
Fire1 Delay 10 10 10
Fire2 Delay 10 10 10
1 = VESDAnet (5) 'Current'
2 = VESDAnet (5) 'Installation'
OK
Cancel
Help

Figure 5-7: Merging two VESDAnets (Device 2)

Fields that have been changed by the merge operation appear bolded in the Target After Merge column.

The merge will not occur until the **OK** button is pressed. If **Cancel** is pressed then all proposed merges are discarded and the original device is left unchanged. Before applying the merge the devices are asked to validate the new settings. If that fails, for example the Action threshold would be set higher than the Fire1 threshold, then the user is warned and the merge prevented.

5.1.4 Single Network Access

VSM4 is designed to work with a pre-defined Monitoring Structure which integrates all connected networks and devices into an integrated system.

VSM4 also supports direct connections to a network for trouble-shooting or other unusual situations. When a direct connection is opened then it will appear in a separate view within VSM4 and require separate login both to VSM4 and to the network/detector to which it is connecting. The network login is required even when the connection is one being monitored since this view is treated completely independently from the Monitoring Structure. Further, opening a separate connection to a network will block the Monitoring Structure from opening the same connection and so should only be done when there is a special need.

This page is intentionally left blank.

6 Administration

This Chapter of the VSM4 Product Guide provides information for administrators to be able to maintain a VSM4 installation.

Areas covered include:

- System Access, including User and Role management. Refer to section 6.1 below.
- Resource Management, including Disk Space monitoring and Backup and Restoration. Refer to section 6.2 below.
- Backup and Restoration. Refer to section 6.2.2 below.
- Software Upgrades. Refer to section 6.3 below.

6.1 System Access

The VSM4 user management integrates access to all the monitored networks and devices so that by logging into VSM4 the user may then have consistent access to all elements of the system, regardless of their connectivity.

VSM4 supports an unlimited number of user accounts. All operators can be clearly defined so that there can be clear traceability between historically logged events and the system operator who was responsible.

Each user is associated with a role or access level. When they logon to the system they may then freely access any function that is rated at or below their access level but are blocked from functions requiring greater access level.

6.1.1 Roles

The roles are:

- **Users -** Access to user level device commands.
- **Administrators -** Access to administrative level device commands, including the ability to modify device configurations.
- **None -** No direct access to the monitoring system, however may receive remote notifications.

All Users

All users, regardless of their assigned role, can perform the following functions without needing to be logged on:

- Receive remote notifications
- Register and Activate the software

Users are not required to provide a username and password in order to browse the available views and settings or connect in read-only mode.

Users can perform the following functions:

- View Configurations
- Open Floor Plans
- View Active Event Lists
- View Events

User Role

User level functions provide similar control to that provided by the buttons on the detector.

The following functions are available at User level:

- Commands such as enable/disable, silence and reset

Administrator Role

In addition to User-level access, Administrators have modify privileges and so can:

- Run Test commands
- Change configurations
- Edit Global Options
- Manage Local Users
- Manage connections
- Close Monitoring Views

6.1.2 User Accounts

User Accounts allow the system to track users and allow the facility manager to control access to the system by explicitly assigning each user a role. User accounts are unrelated to the operating system login accounts.

Users are only able to create, edit or delete accounts with access lower than their own. So Administrators may create accounts at User level and only the Designer can create accounts at Administrator level. All users can modify their own password.

6.1.3 Designer User

The Designer User Account is a unique account which is used by the person responsible for defining the system. The designer user can create and edit floor plans and monitoring structures as described in detail in Chapter 3.

Note: The Designer account should NOT be used for normal monitoring operation. Instead all operators should only work with User or Admin access. This prevents users from inadvertently modifying the monitoring structures and altering the system design.

6.1.4 Create User Accounts

User Accounts allow individuals to access the system and perform their assigned tasks.

1. Log in as an administrator or as the Designer.
2. Select **Security > Manage Users...**

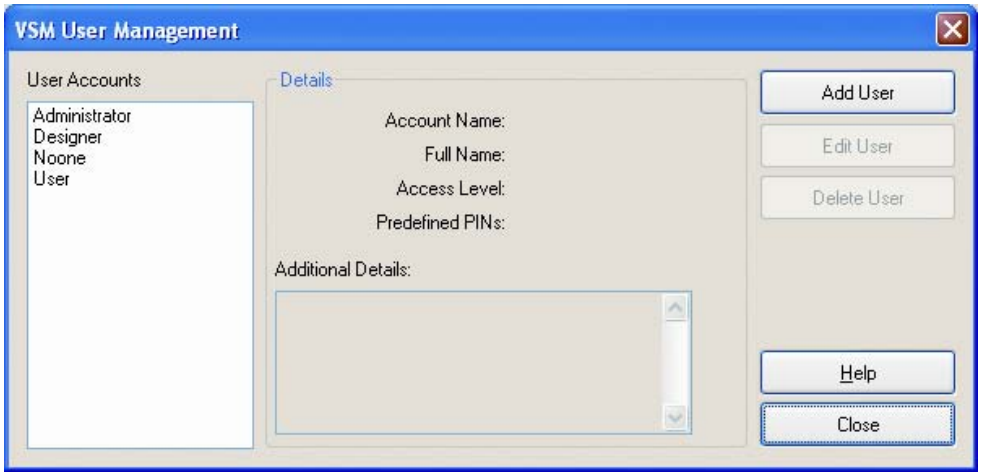


Figure 6-1: User Manager

3. Select **Add User**.

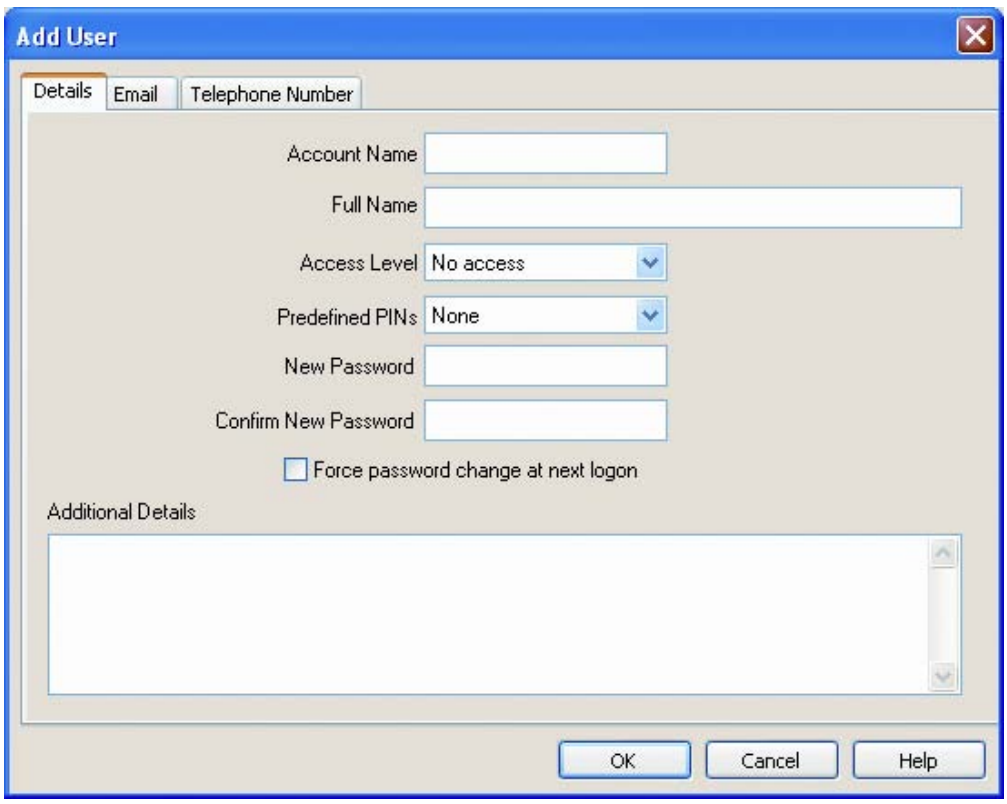


Figure 6-2: Add User

4. Select the **Details** tab.
5. Enter an **Account Name** into the text box. This is the name that will appear on the Status Bar and in the application event log when this user logs on or off the system.
6. Enter the user's **Full Name** into the text box.
7. Select an **Access Level** from the drop down menu.
8. This sets the level of the PINs, as previously defined by the Designer, that may be used by this user. For example, consider a monitoring structure that integrated three VESDAnets where

none of the PINs on the first were predefined, PINs on the second were predefined to User level and PINs were defined up to Admin level on the third connection. In this example, a user who had Predefined PINs set to USER would still have to login to the first VESDAnet but would be able to transparently access USER level functions on the other connections without explicitly logging on to either of them. To access higher level functions, the user must log on at a higher level.

9. Enter a password for the new user into the **New Password** textbox.
10. Re-enter the password in the **Confirm New Password** to confirm the password is correct.
11. Check the **Force password change at next logon checkbox** if you want to force the user to change their password next time they logon.
12. Additional Details: Enter any extra information necessary into the textbox.

If the Remote Notification option is licensed then the Email and SMS tabs will be available:

13. Select the Email tab.

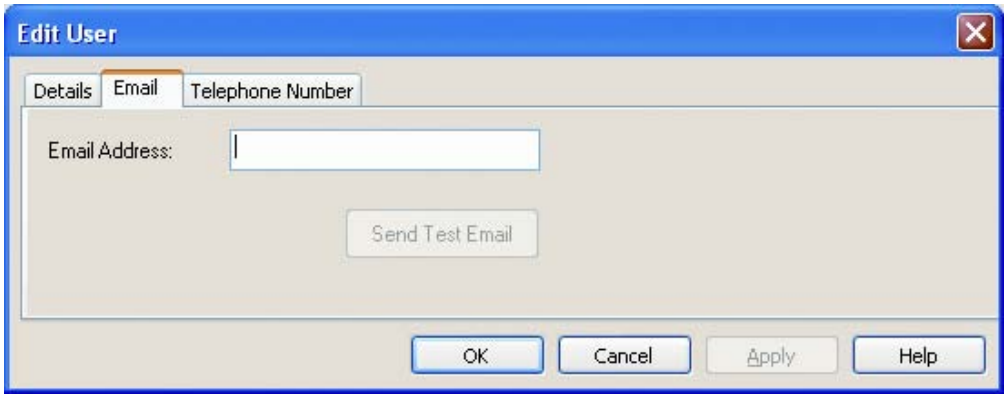


Figure 6-3: Email Tab

14. Enter the new user's email address in the **Email Address** textbox.
15. Click **Send Test Email** if you would like to test the email address you entered.
16. Select the Telephone Number tab.

Figure 6-4: Telephone Tab

17. Enter the new user's telephone number in the **Telephone Number** textbox.
18. Click **Send Test SMS** if you would like to test the telephone number that you have entered.
19. Click **OK** to finish creating the user account.

6.2 Resource Management

6.2.1 Diskspace Monitoring

Diskspace monitoring warns the user when the hard drive is getting full, so that logging events to the database doesn't inadvertently fill the disk completely and halt the application and operating system.

The Diskspace Monitoring Tab of the Options dialog (Figure 6-5 below) is used to set the options for monitoring the available space on the disk volume that VSM4 is installed on.

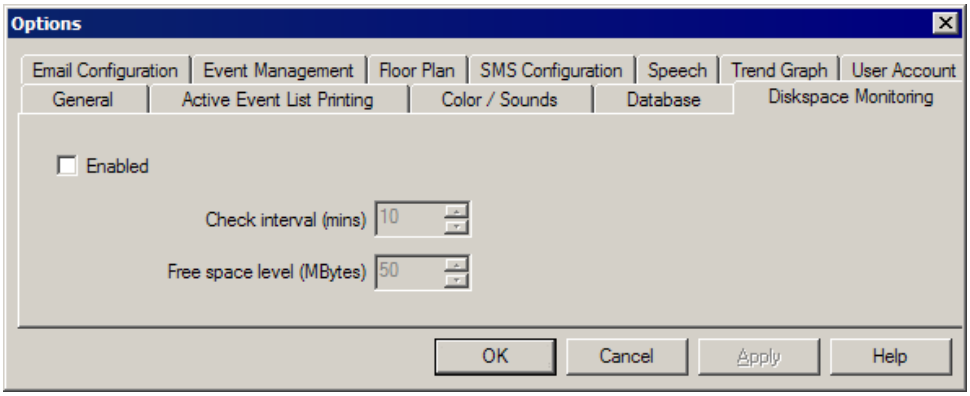


Figure 6-5: View > Options > Diskspace Monitoring

Disk Space Monitoring Settings

- **Enabled -** If the Enabled checkbox is ticked, diskspace monitoring is enabled.
- **Check Interval -** The number of minutes that elapse between each disk space check.
- **Free Space Level -** The level of space on the hard disk, below which a warning message will be displayed.

6.2.2 Backup and Restoration

It is recommended to make backups of settings and data for VSM4, in case of a computer failure or other malfunction. Backups should be made regularly, and when changes are made to the system. Critical items are listed below in Table 6-1.

Item	Default Folder	Process Description
Common System Settings	Windows 7, Vista: C:\ProgramData\Xtralis\Common Windows XP, 2000: C:\Documents and Settings\All Users\Application Data\Xtralis\Common	Backup: 1. Select the Connections, Settings and Event Logs folder. 2. Copy them to a new location, or use your preferred backup software. For example, copy the folders onto a CD. Restoration: 1. Locate your back up copies of the connections, settings and the event log folders. 2. Copy them into the Common folder. 3. Do not replace the SystemGrid.vstyle file.
VSM4 System Settings	Windows 7, Vista: C:\ProgramData\Xtralis\VSM Windows XP, 2000: C:\Documents and Settings\All Users\Application Data\Xtralis\VSM	Backup: 1. Select the Settings and Event Logs folder. 2. Copy them to a new location, or use your preferred backup software. For example, copy the folders onto a CD. 3. Copy them to a new location. For example, copy the folders onto a CD. Restoration: 1. Locate your back up copies of the settings and the event log folders. 2. Copy them into the application data folder.
Monitoring Site and Floor Plan configuration files	Windows 7, Vista: Documents Windows XP, 2000: My Documents	Backup: Use a backup solution to archive the *.vmon and *.vfp files. Restoration: Restore the files and folders to the same location.
Event Log Database - VSM Managed and individual Monitoring Site	Windows 7, Vista: C:\ProgramData\Xtralis\VSM\ Windows XP, 2000: C:\Documents and Settings\All Users\Application Data\Xtralis\VSM\	Backup: Use a backup solution to archive the Managed.db database file. Use a backup solution to archive folders that have the same name as any *.vmon files. Restoration: Restore database files and folders to the same location.
Event Log Database - Custom	User selected.	Consult the database vendor documentation for instructions on how to perform backup operations for that database.
Archived Events	Windows 7, Vista: C:\ProgramData\Xtralis\VSM\EventLogs\dbName.vevt Windows XP, 2000: C:\Documents and Settings\All Users\Application Data\Xtralis\VSM\EventLogs\dbName.vevt	These events have been archived from the working database and should be backed up to longer storage medium. Once backed up they can be deleted as they are no longer used by VSM4. The files can be opened as a standard event log file.

Table 6-1: System, Configuration and Database Backup

Database Archiving

The Database tab of the Options dialog (Figure 6-6) is used to configure the database archiving for all logs.

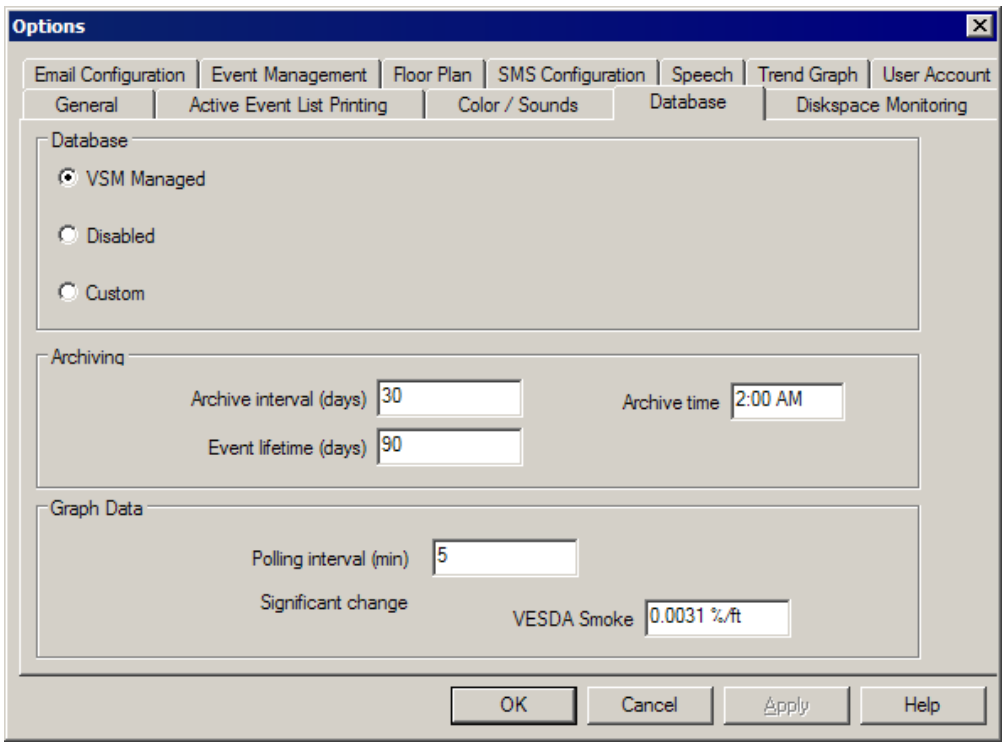


Figure 6-6: Database Options

Archiving parameters include:

- **Archive Interval -** The time between archiving operations.
- **Archive Time -** The time of day that the archiving process is initiated.
- **Event lifetime -** The number of days to keep events in the database before they are automatically deleted. This must be at least as long as the Archive Interval, so that events will be archived before they are deleted from the database.

When events are archived out of the database, they are written to the folder:

Windows 7, Vista:

- C:\ProgramData\Xtralis\VSM\EventLogs\dbName

Windows XP, 2000:

- C:\Documents and Settings\All Users\Application Data\Xtralis\VSM\EventLogs\dbName

where dbName is the (ODBC) name of the database.

They are written as binary eventlog files (with the .vevt extension) in the format:

- n_startDate_endDate.vevt

where n identifies the network, and startDate and endDate are in the format ddmmyyyy.

These archived event logs should be backed up on a regular basis and can be loaded as any other event log file. Once the files are backed up they can be deleted to free up disk space since they are no longer used by VSM4.

6.3 Software Upgrades

Upgrades to VSM4 can consist of:

- installing an updated release.
- adding extra monitoring capacity to VSM4 to support additional devices.

Some upgrades require changes to the licensing and it is important that the person performing the upgrades be familiar with licensing procedures.

To upgrade an evaluation or demonstration license to a full license, or to enable optional features:

1. Contact your authorized Xtralis representative or use the Request License form located in **Help > Register...** to obtain a license code.
2. Input the License Code and select **Activate**.
3. After upgrading a license, such as from a demo to a full license, you must restart the application

To obtain a software upgrade, contact your authorized Xtralis representative. They will supply you with instructions on upgrading your VSM4 installation.

To add extra monitoring capacity to support additional devices:

1. Contact your authorized Xtralis representative to purchase extra tokens.
2. Select **Help > Register**.
3. Enter the new registration code as provided.
4. Refer to Section for more information.

To update the VSM4 software or to migrate from an earlier version:

1. Contact your authorized Xtralis customer service representative to obtain the software.
2. Log into the computer using an account with local administration privileges.
3. Close all software applications.
4. Insert the VSM4 software upgrade installation CD into the CD drive.
5. If autorun is not enabled, locate the VSM4 installation program (VSMSetup.exe) on the CD and run it.
6. Select the VSM4 installation program from the menu system. The InstallShield Wizard should appear.
7. Follow the prompts.

7 Views

VSM4 is designed to monitor all elements of a fire detection system. Several views are provided to allow various aspects of the system to be monitored and controlled. Although the views are described in earlier chapters they are covered in detail here.

The views are:

- **Active Event List -** This view displays all active events. Refer to section 7.2 for further information.
- **Status Bar -** This view highlights the highest priority event in the system. Refer to section 7.3 for further information.
- **Floor Plan -** This view displays the location of zones and devices in relation to a hierarchy of floor plans. Refer to section 7.4 for further information.
- **Browser -** This browser view displays HTML pages corresponding to the active condition on the currently selected floor plan. Refer to section 7.5 for further information.
- **Status View -** This view displays detailed status for a specific device. Refer to section 7.6 for further information.
- **Monitor Browser -** Integrates multiple networks into a logical structure to provide a network-centric view of the system. Refer to section 7.7 for further information.
- **Device View -** Displays all devices associated with an individual connection. It is similar to the Monitor Browser without logical nodes.
- **Trend Graph -** This view displays line graphs of the state of detectors and outputs. It can track live data changes. Refer to section 7.9 for further information.
- **Event Log -** This view displays logged events. Refer to section 7.10 for further information.

7.1 Common Behaviour

Most views represent or reference devices, whether as a node in a tree, an entry on the Active Event List, a region on a floor plan or an entry on the legend of a graph. Each representation of a device supports a context menu to allow the user to bring up other views of the device or to issue commands to that device. If a device drops offline then its commands will be hidden.

Devices nodes on a tree and rows on the grid may be dragged between views. For example, rows on a Monitor Browser grid representing devices can be dragged onto a graph. The clipboard cut/paste operations may be used in all places that are supported by device drag and drop operations. Clipboard actions may also be used to export text from grids to spreadsheets and text editing programs.

Views have specialized commands and these appear as a menu positioned immediately following the main View menu. Most views also display a toolbar that sits at the top of the frame, but may be dragged elsewhere. These toolbars and menus are only shown when the view has focus. Some views may be persisted to file and in these cases they support a Save and Open menu command. Many views also support the Print command.

7.2 Integrated Active Event List

The Active Event List provides a prioritized list of all active conditions within the system which serves as a quick summary of the state of the entire system. The alarms and troubles are sorted so that the highest priority conditions appear at the top of the list.

7.2.1 Active Event List

The simple Active Event List is similar to the Integrated Active Event List but applies only to a specific network connection and lists only the active conditions that are current for that network. If the connection is lost then this view is automatically closed.

The event counter in the status bar shows how many events are displayed in the table (see Figure 7-1).

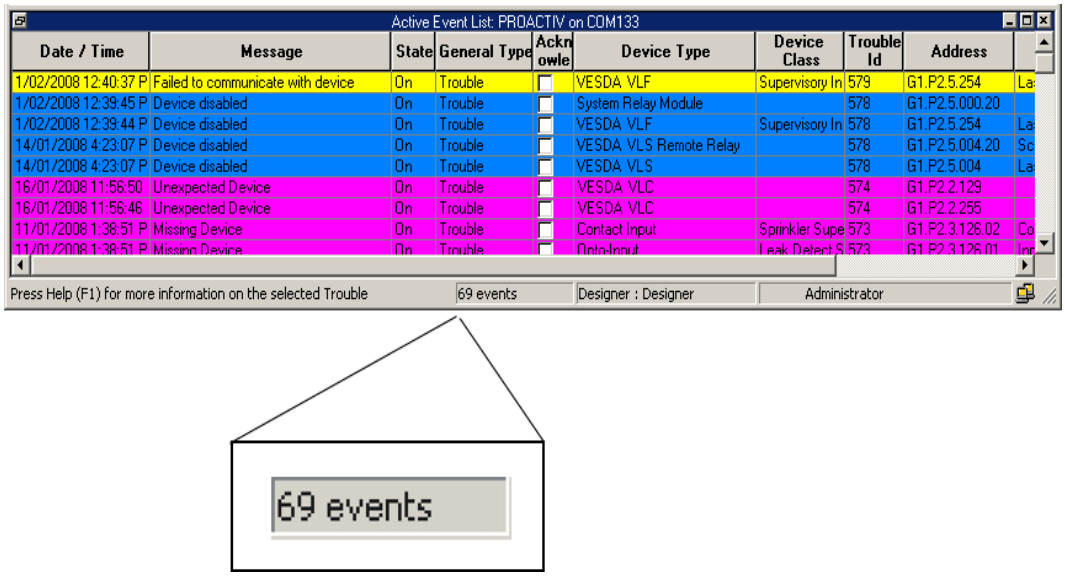

Active Event List: PROACTIV on COM133
Date / Time
Message
State
General Type
Acknowle
Device Type
Device Class
Trouble Id
Address
1/02/2008 12:40:37 P Failed to communicate with device On Trouble VESDA VLF Supervisory In 579 G1.P2.5.254
1/02/2008 12:39:45 P Device disabled On Trouble System Relay Module 578 G1.P2.5.000.20
1/02/2008 12:39:44 P Device disabled On Trouble VESDA VLF Supervisory In 578 G1.P2.5.254
14/01/2008 4:23:07 P Device disabled On Trouble VESDA VLS Remote Relay 578 G1.P2.5.004.20
14/01/2008 4:23:07 P Device disabled On Trouble VESDA VLS 578 G1.P2.5.004
16/01/2008 11:56:50 Unexpected Device On Trouble VESDA VLC 574 G1.P2.2.129
16/01/2008 11:56:46 Unexpected Device On Trouble VESDA VLC 574 G1.P2.2.255
11/01/2008 1:38:51 P Missing Device On Trouble Contact Input Sprinkler Supe 573 G1.P2.3.126.02
Press Help (F1) for more information on the selected Trouble
69 events
Designer : Designer
Administrator
69 events

Figure 7-1: Event Counter

7.2.2 Toolbar

The Active Event List toolbar is shown below.

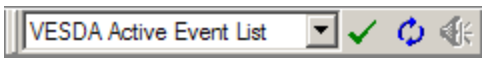


Figure 7-2: Active Event List Toolbar

Select Table Style

The Active Event List comes with predefined table styles depending on the network or source of the list. The table style defines which data fields are shown in the table and the order in which they appear The Grid Style Manager allows the user to define additional styles and to edit their own styles.

Note that the user cannot change the sort order of an Active Event List, as the highest priority conditions will always appear at the top of the list.

The event priority and the Acknowledge and Latching behavior are described in Section 4.3.

Acknowledge

This command is used to inform the system that the user has been made aware of this condition and has acknowledged it. If the event has already been acknowledged then this command is disabled.

Reset

Resets the detector which clears events. If the conditions continue to exist then they will be regenerated. This command will be disabled if the event relates to a non-detector type trouble such as a 'Lost connection'.

Silence

Silences outputs on the device associated with the event. This button can be toggled to 'un-silence' a silenced device.

7.2.3 Event List Menu

This is the main menu that is associated with the Active Event List and which corresponds to its toolbar (shown below).

7.2.4 Context Menu

Clicking the right mouse button on a condition in the Active Event List will bring up the shown context menu. Most of the options relate to the device associated with the selected condition. Only the Help option is enabled if more than one condition is selected in the list.

- **Help -** Provides a summary description of the condition and possible responses.
- **Edit -** Selecting this option will bring up the property pages for the device. This can be useful for inspecting threshold levels or flow rate settings.
- **Device -** This is a cascaded menu that contains all commands for the device.
- **View -** This is a cascaded menu that provides access to all views related to the device.

7.2.5 Double Clicking

Double clicking on a condition will bring up the Device Status View for the associated device. For example double clicking on an air flow fault on a VLF would bring up the Device Status View for that detector.

Active Event List Printing Options

The Active Event List Printing Tab of the Options dialog (Figure 7-3) is used to set automatic printing options for a line printer.

Each print job contains details of the event and spans two lines.

Note: Event printing requires a line printer.

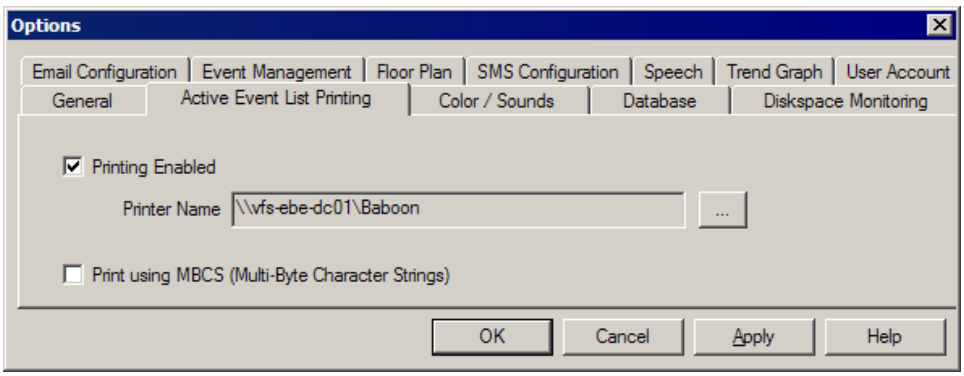


Figure 7-3: View > Options > Active Event List Printing

Printing Settings

- **Printing Enabled -** Check to enable automatic printing of an incoming event notification. Select the browse button to select a printer. If the printer is not on the list, add it using the

Windows Add Printers program (**Start > Settings > Printers and Faxes** in Windows XP). The printer you have selected is displayed in the Printer Name textbox. The printer must be a line printer.

- **Print using MBCS (Multi-Byte Character Strings) -** Check if printing MBCS text (for example, you are printing Chinese characters).

  If the realtime printing does not reproduce the correct character set, check whether the printer supports MBCS rather than the more common Unicode character set. If so, check this option.

7.2.6 Grid Style Manager

The Active Event List comes with predefined table styles depending on the network or source of the list. The Grid Style Manager allows the user to define additional styles and to edit their own styles.

Note: System styles may not be edited but may be used as the basis for a user style which can be edited.

The style defines which columns are shown in the table, the order of the columns and the width of the columns and which columns are used as keys when sorting the table.

Note: The user cannot change the sort order of an Active Event List, as the highest priority conditions will always appear at the top of the list.

Once a style is defined then it can be selected in the combo box on the toolbar.

Figure 7-4: Style Menu

Creating a New Style

Open the style manager by selecting ***View*** **> Grid Style Manager**.

Note: The View Menu will depend on the actual view, for example, for the Event Log the menu command is found at **Event List > Grid Style Manager**.

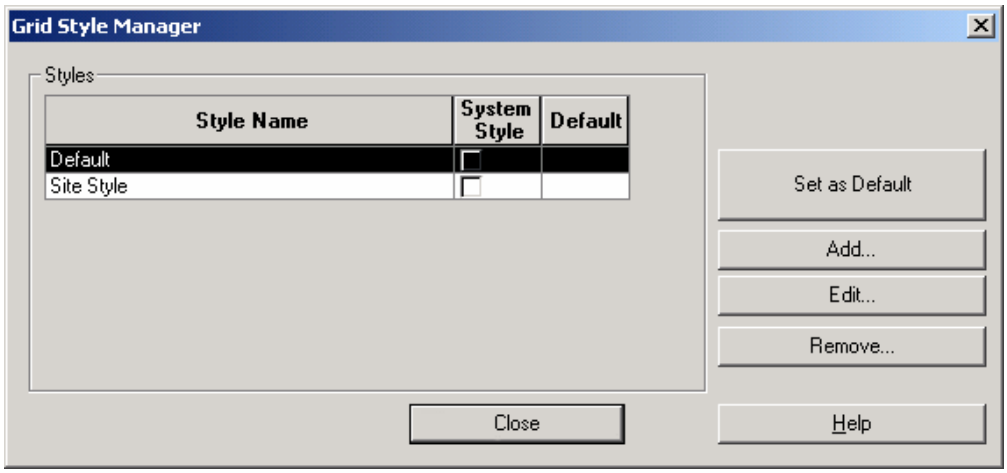


Figure 7-5: Grid Style Manager

Select the style that you want to use as a basis.

Click on the **Add…** button. The style should first be given a meaningful name.

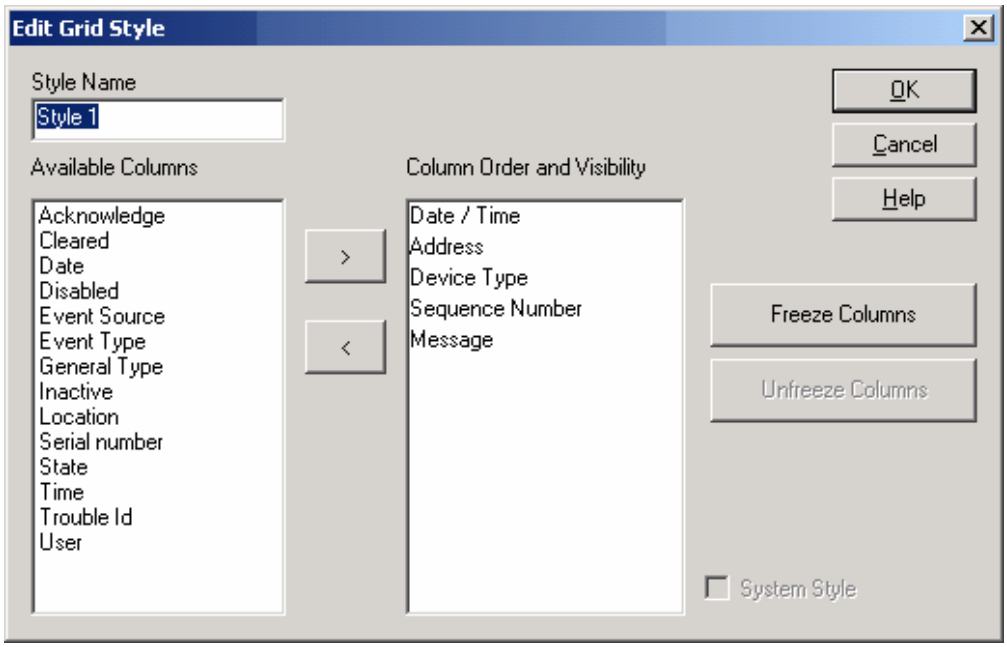


Figure 7-6: Edit Grid Style

The dialog shows the columns that will be visible in the right list; the left list shows other possible columns. The order in the right column can be changed by dragging the entry to the desired position.

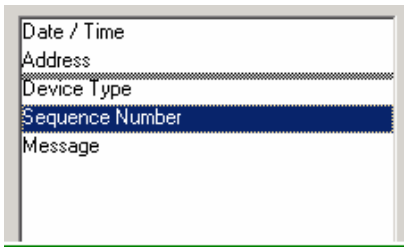


Figure 7-7: Grid Style Column Selection

Freezing columns refers to those columns that remain 'frozen' in place when scrolling to the right on the grid. To freeze some columns select the last column to be frozen and click on **Freeze Columns**. The frozen columns will then appear in bold.

Set the column widths by first closing the Grid Style Manager and selecting the style in the combo box, then resizing the columns by clicking on the separator to the right of the column heading and dragging it. Double clicking on the right separator will set the column width to that of the widest data field in the column.

Clicking on a column heading in the table will cause the data to be sorted in ascending order based on the value of that column. Clicking again on the same column will toggle the sort order to descending order. If multiple rows have the same value for the current sorting column then the previous sorted column is used to order them. For example, if an event log was sorted on time and then was sorted on event category, then the events would now sort on category but where there were multiple events with the same category, for example troubles, they would be sorted on time.

The table style is saved when the application is closed.

7.3 Status Bar

The Status Bar always sits at the bottom of the main frame and shows key information about the highest priority condition in the system. Its prominence and simplicity ensure that an operator is made aware of crucial events.

The Status Bar shows the highest priority event on the Active Event List. Refer to section 4.2 for information on the prioritization system that it uses.

Figure 7-8: Status Bar

7.3.1 Contents

The device location and the event message sit in the middle of the status bar and are shown in large font. The time-stamp, device type and address appear to the left in normal font. On the right are the Acknowledge, Reset and Silence buttons.

7.3.2 Acknowledge

This button is used to indicate that the user has been made aware of this condition and has acknowledged it. If the event has already been acknowledged then this button is disabled. The status bar will flash while an event is unacknowledged to get the operator's attention.

7.3.3 Reset

Resets the detector which clears events. If the conditions continue to exist then they will be regenerated. This will be disabled if the event relates to a non-detector type trouble such as a 'Lost connection'.

7.3.4 Silence

Silences outputs on the Xtralis fire system. This button can be toggled to 'un-silence' a silenced system.

7.3.5 Actions

- **Double Click -** The Status Bar can be configured to respond to a double click by bringing up the Device Status view or/and causing the Floor Plan view to select the floor plan containing the detector associated with the active event on the status bar. The response settings are on the Floor Plan tab on the **View > Options** menu.

7.4 Floor Plan

The Floor Plan view shows where issues occur and the location of detectors (and other devices). Hence when a detector senses smoke the floor plan will show whether the condition is limited to that detector or is affecting the surrounding detectors.

The Floor Plan view displays a location hierarchy on the left, while the right side shows the 'floor plan' for the node selected in the tree.

7.4.1 Navigation

Navigation around the floor plan structure is typically via double clicks on active regions that are hyperlinked to other floor plans. Most active regions represent sub-regions of the current floor plan, but it is also possible to hyperlink to completely separate branches of the floor plan tree. Of course the selected floor plan can also be changed by explicitly selecting another node in the tree.

Selecting **Floor Plan > Back** (or the equivalent toolbar button) will undo the selection changes. This is also the first command on the context menu. Up to 16 selection changes can be undone.

Double-clicking on an active region that represents a device will bring up its Status view which shows measured trends and detailed status for that device.

Zoom

The Floor Plan provides several functions to allow the user to define what area of a floor plan to view. The Zoom In/Out functions on the menu and toolbar do the standard zoom operations based on the centre point of the view. The Zoom window option changes the cursor to show a window symbol below the arrow. Drag out a rectangle to define the region you wish to view and VSM4 will optimize the zoom and pan to show that region.

The Show All option sets the zoom to just include the entire floor plan in the view.

Navigator Tool

Select the **Floor Plan > Navigate** menu (or click on its icon) to invoke the Navigator tool (Figure 7-9).

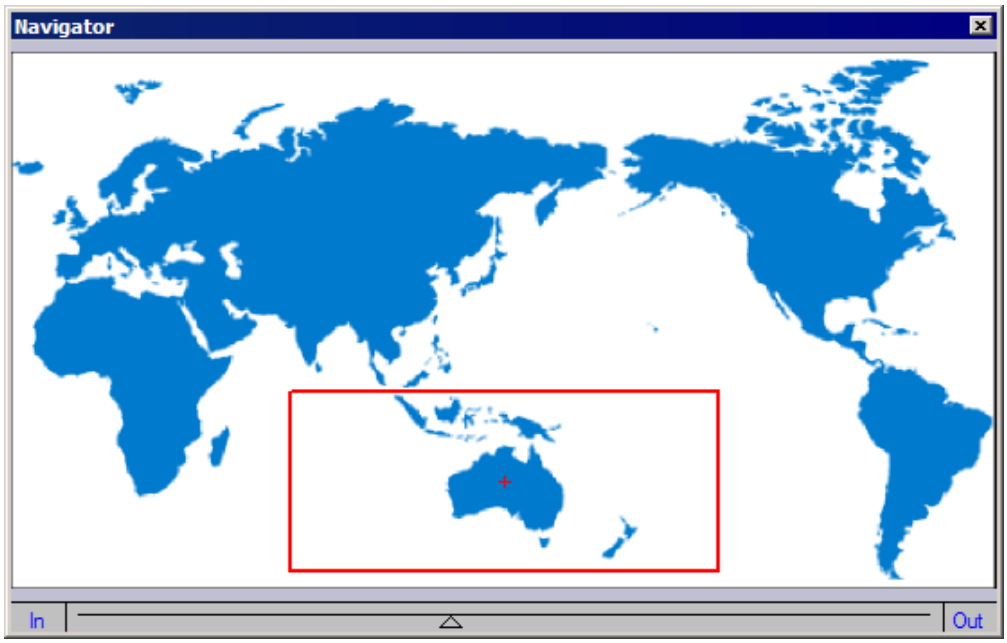


Figure 7-9: Floor Plan Navigator

The entire picture is shown greatly reduced, in this tool, with the region shown on the Floor Plan view represented by a red rectangle. The red rectangle can be moved around to show different regions on the main view. The slider can be moved to change the zoom factor. This tool is especially useful when zoomed into a small region on a large floor plan since it provides context and allows very rapid movement around the plan.

Automatic Selection

The Floor Plan can be configured to update when a new alarm (or pre-alarm) occurs (that also becomes the highest priority event). This property is enabled on the Floor Plan tab of the Options dialog.

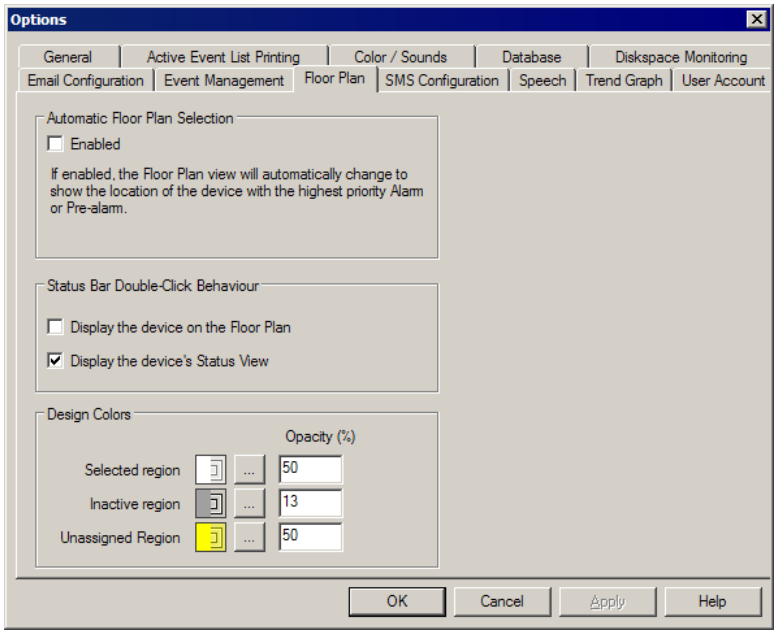


Figure 7-10: Floor Plan Options

While viewing the floor plan for one alarm it is possible that another alarm will occur and change the selection. This can be prevented by selecting the **Floor Plan > Locked** menu. This lock can be removed by selecting **Floor Plan > Locked** again, or by just changing the selection.

Selection

Selecting a floor plan node in the tree will cause that floor plan to be shown. Selecting a hyperlink node in the tree will cause the relevant floor plan to be shown and the shapes associated with the link to be highlighted. This highlighting is subtle since it is constrained to not change the color (since color is used to indicate a condition) and it still needs to allow the region to flash. Consequently, the selected shape(s) will appear slightly brighter than those that aren't selected.

When a shape is selected in the floor plan then its boundary is shown as a dashed line. If the shape is associated with a link then the link-node in the tree will also be shown as selected, otherwise the floor plan node in the tree will be shown as selected.

7.4.2 Device Hyperlinks

When an active region is selected in the floor plan that corresponds to a device, or if its tree node is selected, then the property pages for the device may be viewed using the **View > Device Configuration**… menu. These properties are also accessible through the **Edit > Edit** menu while in monitoring mode.

The icon and tree text and the tooltip for a link will all be that of the target device. Links to other floor plans will show the location string of the floor plan and trouble indications but they have a distinct icon ( ) so that they aren't confused with Floor Plans.

If the target is removed then the tree node will appear as ( ) where the text to the right of the arrow indicates the address of the missing target. In this case 'tst' was the abbreviation of a location in the floor plan that was deleted.

7.4.3 Overlapping Shapes

When multiple detectors are monitoring the same region then their shapes overlap. This is a valid situation that where multiple detectors can be used independently to confirm a fire before suppressant can be released. Clicking with the mouse on this overlap will cycle through each of the shapes changing their drawing order. The tooltip corresponds to the current shape.

7.4.4 Unassigned Devices

If the designer has created shapes but not assigned them to a link then they will not be shown while monitoring. However, when the mouse cursor moves over the top of them then they will show a tooltip of 'Unassigned'.

7.4.5 Building a Location Hierarchy

Note: The following design operations are only accessible once the user has logged on as the Designer.

A Location hierarchy will normally be created by first setting up a Monitoring Structure and then selecting the **View > Floor Plan** menu as described in Chapter 3. This sequence will also associate the created Floor Plan with the Monitoring Structure. An alternative is to go the other way and first create a Location hierarchy using the **New > Location** menu and then create and link the Monitoring structure by selecting the **View > Monitor Browser** menu.

Once a location hierarchy exists then it can be extended by inserting Floor Plans under any existing level. As each Floor Plan is added it should be edited to give it a meaningful name and abbreviation. The Floor Plan tab in its property pages should be edited and an image or CAD file imported.

Before importing CAD files, strip out irrelevant details. This may include layers that were for construction but not relevant to the operators or it may contain fine detail; you don't really need to see every bolt or bracket in the building when monitoring fires. Stripping out irrelevant details reduces the size of the CAD files which speeds up their loading and display. A good rule of thumb is to keep the size below 1 Megabyte.

7.4.6 Structure of Floor Plan Files

When images are imported they are integrated into CAD files so that VSM4 can define active regions and other annotations in a layer (titled 'VSC') that sits above the image. It is the regions in this layer that change color and flash when the zone is in trouble or alarm. The shapes in the 'VSC' layer should never be edited by other tools. Editing of other layers should have no affect on VSM4.

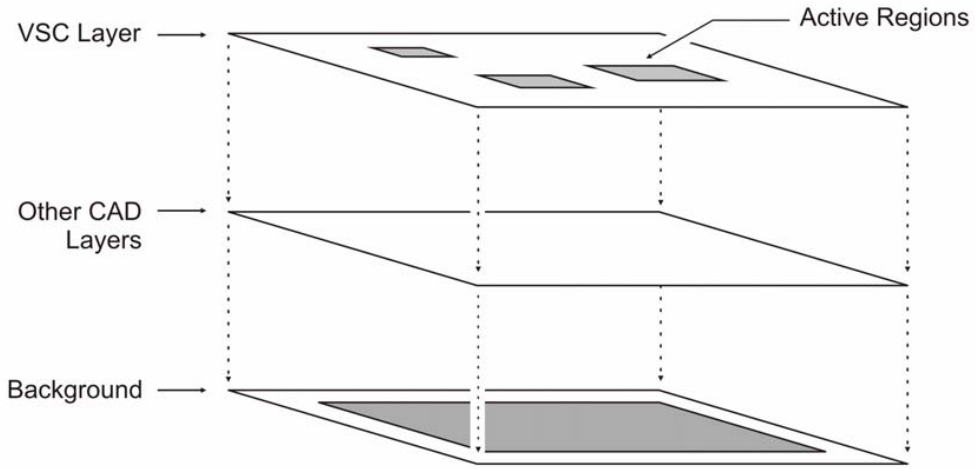


Figure 7-11: Floor Plan CAD Layers

7.4.7 Defining Links

Hyperlinks tie active regions on a floor plan to a device in a monitoring structure, or to another Floor Plan. Creation of links is a two step operation.

1. Create the shape(s) using the **Edit > Insert** menu when the right side of view is selected (or use the Insert on the context menu). The Insert options are detailed below.
2. Drag and drop the target node onto the shape. When this happens the first time then a Link node is created on the tree to represent this hyperlink.

If there are multiple regions representing the same device then the remaining regions can be linked by Drag and dropping the target node onto each of the regions. Alternatively, the Link node (in the Floor Plan tree) can be dragged onto each of the remaining regions.

7.4.8 Icons

Dragging and dropping a device onto a background section (i.e. away from any shapes) will cause the device's icon to be drawn at that location. The icon will show the same state as the icon on the tree and will flash if any troubles or alarms occur.

7.4.9 Propagation of Events

When a device is not linked to a floor plan, any troubles or alarms occurring on this device are fed to its container. If the container is not represented on the floor plan then the events will propagate further up the network tree (see Monitoring Browser, section 7.7). Consequently, it is good practice to include an icon or a region on the Floor Plan in order to catch any troubles (or alarms) for any of the devices that it monitors.

7.4.10 Creating Shapes

A range of shapes are provided to allow virtually any shape to be created to described a region on an image or floor plan. These are found on the floor plan context menu cascaded under the Insert sub-menu.

Rectangle

Cursor changes to a cross-hair.

1. Click left mouse button at desired corner of rectangle.
2. Moving the mouse will drag out a rectangle. Click mouse button again when the rectangle is the desired size.

Polyline

Cursor changes to .

1. Click left mouse button at desired starting point.
2. Move mouse to define first line segment and click mouse at end of segment.
3. Keep defining segments until shape is defined.
4. Right click on mouse and select Enter. (Enter Closed or Enter Polygon do essentially the same thing).

If the shape being defined requires arcs, define the linear segments as described above in steps 1-3 and then when you require an arc, right click and select Arc from the context menu. All subsequent segments will be arcs until you select Line from the context menu. The polyline context menu also supports an Undo option which will remove the last segment. It can be repeated until all segments have been undone.

Polygon

When this is selected you will be prompted with the following dialog:

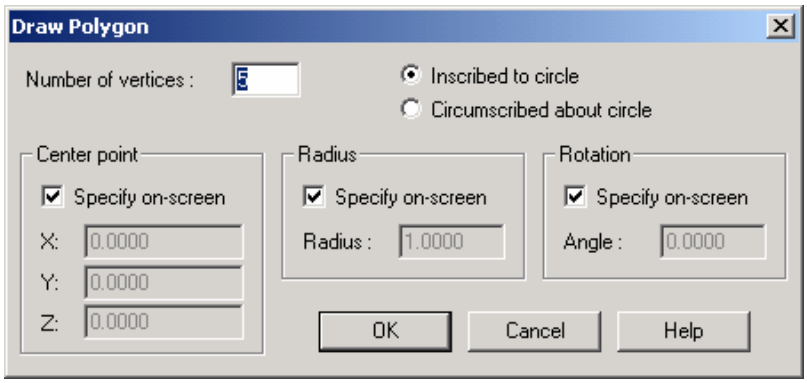
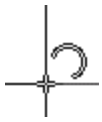


Figure 7-12: Draw Polygon

The key setting here is the number of vertices. The default values on the other settings allow the size and angle to be interactively defined.

1. Specify the number of vertices and click on **OK**. The cursor changes to .
2. Move the cursor to where the center of the polygon should be located and click the left mouse button.
3. Move the mouse this will cause the polygon to grow and rotate so that a vertex is always attached to the mouse. Click the mouse button again when the polygon is of the correct size and rotation. (If you have not got the angle, size or location exactly correct, don't worry since these can be modified as described below under Editing Shapes).

Arc

The cursor will change to a cross-hair and  .

1. Click on the start of the arc.
2. Click on a point along the arc to define the curvature of the arc.
3. Click on the end of the arc.

Right clicking cancels the arc insertion.

Circle

The cursor changes to a cross-hair and a circle.

1. Click on the left mouse button to indicate the centre of the circle.
2. Move the mouse and the circle will grow so that the circumference will follow the mouse. When the circle has the correct size and position then click the mouse button again.

Right clicking cancels the operation.

Ellipse

The cursor changes to a cross-hair and an ellipse.

1. Click on the left mouse button to indicate the centre of the ellipse.
2. Move the mouse to where the minor or major axis touches the ellipse boundary.
3. Move the mouse and the ellipse will grow so that the boundary will follow the mouse. When the ellipse has the correct size and position then click the mouse button again.

Right clicking cancels the operation.

Image

This is used for adding annotations to a floor plan.

Note: It should NEVER be used for loading in the floor plan image. It is recommended that it only be used for adding standard annotations such as Fire Doors, Extinguishers etc.

Images should NOT be linked to devices since they won't flash like other shapes if a trouble or alarm occurs on that device.

To add an image:

1. Browse to the image file.
2. The user will be prompted with the dialog below.

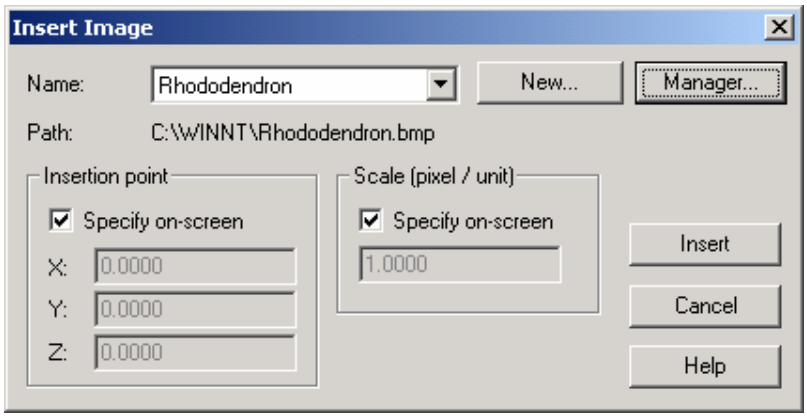


Figure 7-13: Insert Image

3. The **New…** button allows the user to change the image and the **Manager…** button shows properties of the image, as well as a view of it. Usually these should not require change. Click the **Insert** button when ready.
4. The cursor changes to a smiley face . Click on the where you want the lower left of the image to be placed.
5. Move the mouse and an image box with the correct aspect ratio will be drawn above and to the right of the first click. Click when the correct size has been reached.

Right clicking cancels the operation.

Spline

1. Click at the start of the spline.
2. Move the mouse to the next point and click again.
3. Repeat until the shape is defined and then right click and select Enter Closed (Enter Polygon has the same effect) from the context menu. Don't use 'Enter'.
4. Move the mouse to define the correct tangent for the joining point and then click the mouse button again.

Like Polyline, this operation supports Undo.

7.4.11 Drawing Annotations

- **Line -** This just keeps adding lines until you right click. You can not build up shapes this way but the lines could be used for annotations.
- **Multiline -** This draws parallel lines but does not create a 'shape' from them that is used by VSM4 so only use for annotations.

7.4.12 Editing Shapes

If the shape is not quite correct then right click on it and select Move, Rotate, Scale from the context menu. If this is not sufficient then you can always delete it and re-create it.

Right clicking in the middle of these operations will cancel the operation.

Delete

Right click on the shape and select Delete.

Move

1. Right click on the shape to be moved and select Move from the context menu. The cursor will change to a cross-hair.
2. Click with the left mouse button on the shape.
3. Move the mouse and the outline of the shape will be moved with the mouse. Click again when you reach the correct position.

Rotate

The cursor changes to .

1. Click on the point around which you wish to rotate the shape. (Note: this does not even need to be on the shape – but it is usually more intuitive if it is).
2. Move the mouse and the outline of the shape will rotate to follow it. Click again when you achieve the correct orientation.

Scale

The cursor changes to a cross-hair and .

1. Click on a point. (Note: this does not need to be on the shape).
2. Move the mouse and the outline of the shape will scale by the distance of the mouse from the first point. Click again when you achieve the correct size.

Mirror

The cursor changes to a cross-hair and .

To define the mirror line:

1. Click on a point on the 'mirror-line'.
2. Move the mouse and the mirror line will follow it and the outline of the reflected shape will also be shown. Click again when you achieve the correct reflection.

7.4.13 Editing Hyperlinks

The Link node in the tree to represent a link has a similar property page to other nodes in the tree but there are two differences.

1. It shows the address of its target node (as a read-only) field.
2. It has an override checkbox next to its location string. When this is checked then the location that is shown for this node on the tree or in the tooltip text on the floor plan will use the link's location string rather than that of the target. This is useful for devices that don't have a location such as a scanner sector.

7.4.14 Options

Colors

While in Designer mode the shape colors are based on whether:

1. the shape is yet to be assigned (i.e. is still Unassigned)
2. the shape is assigned whether it is selected in the tree (Selected) or is Inactive.

Each of these colors can be defined on the Floor Plan tab of the Options dialog to enable the designer to pick colors that stand out against the images or floor plan CAD files that they are using.

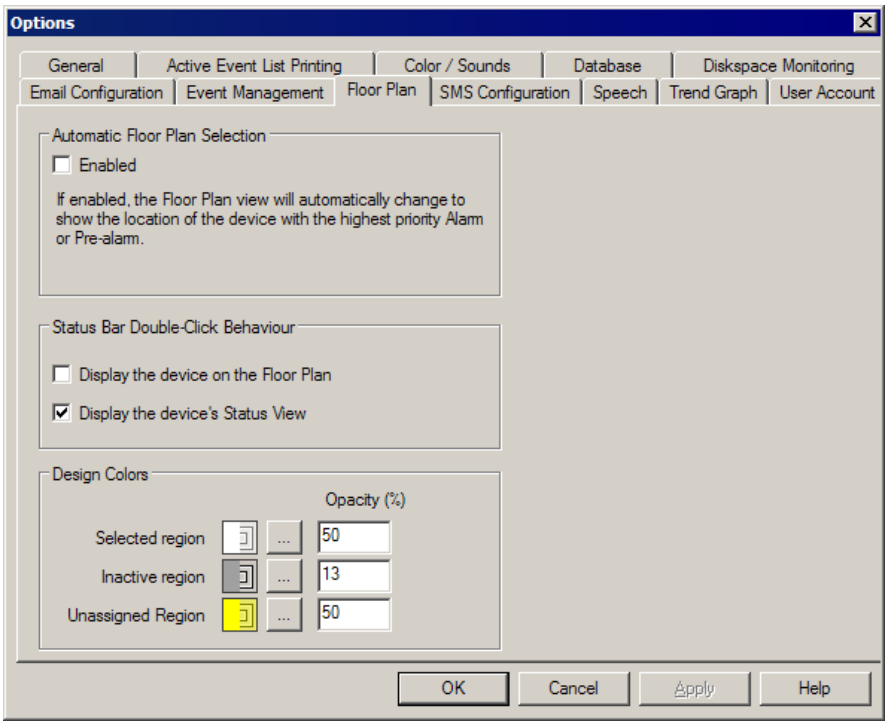


Figure 7-14: Floor Plan Options

7.4.15 Customization

The templates for the text on the tree nodes and the text on the floor plan tool tips can be customized using the Customize commands on the menu. However, these menu items are only available when the Designer is logged on and working with the Floor Plan in Design mode.

Customize Tree Node Text

The text for the tree nodes can be customized using the menu **Floor Plan > Customize Tree Text**. The dialog, shown below, allows the text to be defined as a template. The template field shows parameters in blue and literal text in black.

- Parameters are added by placing the cursor at the desired insertion point and then clicking on the parameter in the Available Parameters list.
- Text can be removed from the template using the **Delete** key. Deleting any part of a parameter name will delete the entire parameter.

The Sample Format shows the output for the root node of the floor plan tree.

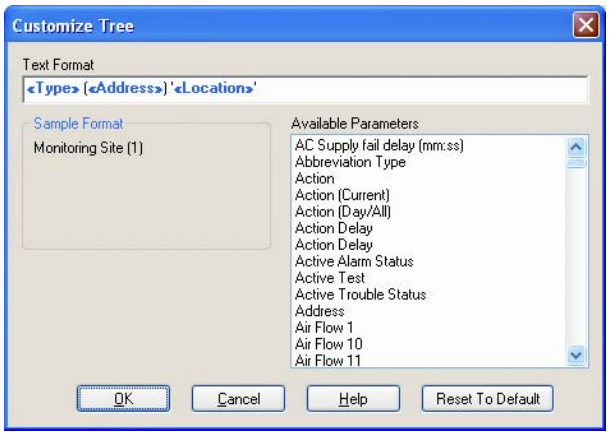


Figure 7-15: Customize Tree

Customize Tooltips

The tooltips, that are shown when the mouse hovers over active regions on the floor plan, are based on a template. The template is edited using the menu **Floor Plan > Customize ToolTips**. This brings up a window like that shown above.

To insert a line break in the tooltip text, insert a backslash followed by n (i.e. \n).

7.4.16 Verification Warnings

The Verification tool will report warnings for the following.

- **The link node xx is not associated with any regions or icons on the floor plan yy -** This advises the user that the link is doing little and while the node in the tree will change state there is nothing on the actual floor plan that will change.
- **There are unassigned regions on the floor plan yy -** Regions have been created on the floor plan that are not linked to a device or another region. This usually indicates an oversight by the designer.
- **The input device does not appear on the floor plan -** A detector on one of the monitored networks is not linked to any of the floor plans.
- **The input device appears on n floor plans -** While this may be valid, e.g. a detector monitoring a stairwell that spans multiple floors, it generally indicates that this device is appearing in at least one floor plan where it shouldn't.
- **The hyperlink has no device associated with it -** This indicates that the target for this link has been removed. It is important to understand what has caused this, especially if it is a

detector that has dropped offline. If the target is never going to re-appear then remove the link. This warning is only given when running in Designer mode.

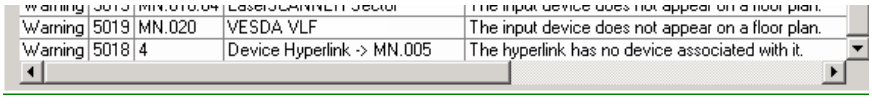

Warning 5019 MN.020 VESDA VLF The input device does not appear on a floor plan.
Warning 5018 4 Device Hyperlink -> MN.005 The hyperlink has no device associated with it.

Figure 7-16: Verification Warnings

7.4.17 Active Event List Warnings

If a device goes missing that is pointed to by a link then an event will be placed in the Active Event List.

15/06/2007 12:26:27 PM MN.001 Major low air flow pipe 1 VESDA VLP
15/06/2007 12:28:07 PM Device hyperlink 'A1.B2.Device Hyperlink -> MN.005' references missing device at address 005

Figure 7-17: Active Event List Warnings

7.5 HTML Browser

The Browser shows the user document(s) that describes responses to active conditions in the current floor plan. The content of these documents will usually be provided by the site and integrated with the floor plans by the Designer. The operator should be familiar with these procedures and trained to refer to them when an incident occurs.

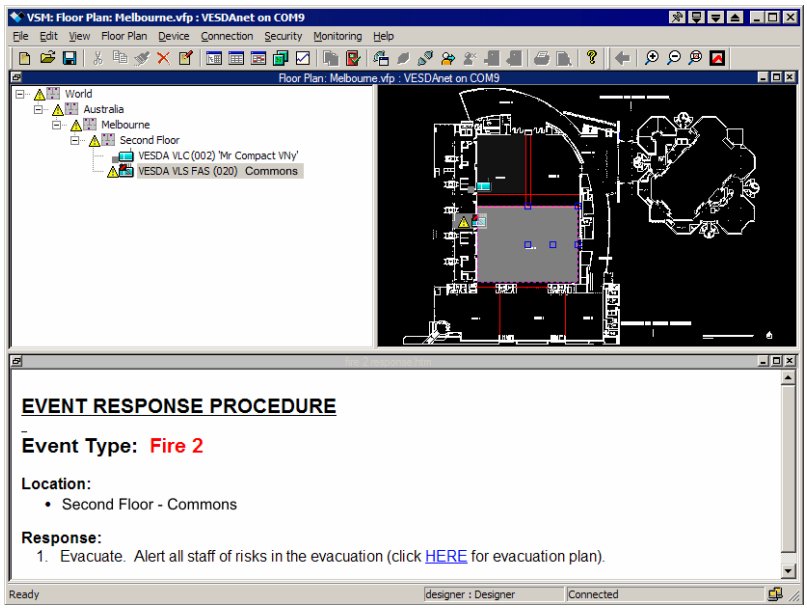

VSM: Floor Plan: Melbourne.vfp : VESDAnet on COM9
File Edit View Floor Plan Device Connection Security Monitoring Help
Floor Plan: Melbourne.vfp : VESDAnet on COM9
World
Australia
Melbourne
Second Floor
VESDA VLC (002) 'Mr Compact VNy'
VESDA VLS FAS (020) Commons
EVENT RESPONSE PROCEDURE
Event Type: Fire 2
Location:
Second Floor - Commons
Response:
1. Evacuate. Alert all staff of risks in the evacuation (click HERE for evacuation plan).
Ready
designer : Designer
Connected

Figure 7-18: HTML Browser

VSM4 supports linking response documentation to zones, thus providing instant context-relevant information to the operator when an incident occurs. This can warn the operator of specific dangers associated with an area, such as the presence of dangerous chemicals or it can remind them of standard site operating procedures. The Designer will usually take documentation associated with locations and condition responses provided by the end user and link these into the Floor Plan structure that has been created.

Documents that detail response procedures can be linked to specific locations and customized for specific event types. Any HTML page that can be viewed in Microsoft Internet Explorer may be referenced.

Many modern document authoring applications can export documents to HTML. It is also possible to link to animated HTML pages or event to web cameras.

7.5.1 General Responses

VSM4 allows the Designer to define responses specific to a given location and event type while also allowing the Designer to specify general policies and procedures.

During monitoring, the HTML documents are displayed in response to the events that they are linked to. If there is a HTML page defined for the event and its location then it is used. However, if there isn't a URL specified for the event type/device combination then the parents of the device in the Floor Plan are checked for a URL of the same event type. If no match is found there then the parent's parent is checked until a match is found or the top of the tree is reached.

Each event type can refer to separate documents, or if the complexity of the site does not require a lot of detail for each procedure, all procedures can be placed on a single document. Advanced users can then utilize bookmarks to open the document to a specific location within the overall document for each event type.

7.5.2 Response Content

Expected event responses are:

- **Fire events -** should describe evacuation procedures and the locations of hazards.
- **Supervisory and Trouble events -** contact details for a sufficiently trained person in order to diagnose and correct a fault or carry out the required process, for example a filter change.

7.5.3 Response Definition Procedure

To associate Procedure Documents with Floor Plan elements:

1. Log in as the Designer User.
2. Open the Floor Plan and select **Floor Plan > Designer Mode**.
3. Click on the Floor Plan view and then select **View > Browser** to open up the HTML browser.
4. Right-click over any item listed in the Floor Plan, select **Edit** from the context menu and then the Browser tab.
5. Enter a file location or an internet address (URL) for each event type (refer to Figure 7-19 below).
6. Select **Test URL** to ensure that VSM4 can read the document correctly. The Browser must be open to enable this to work correctly.

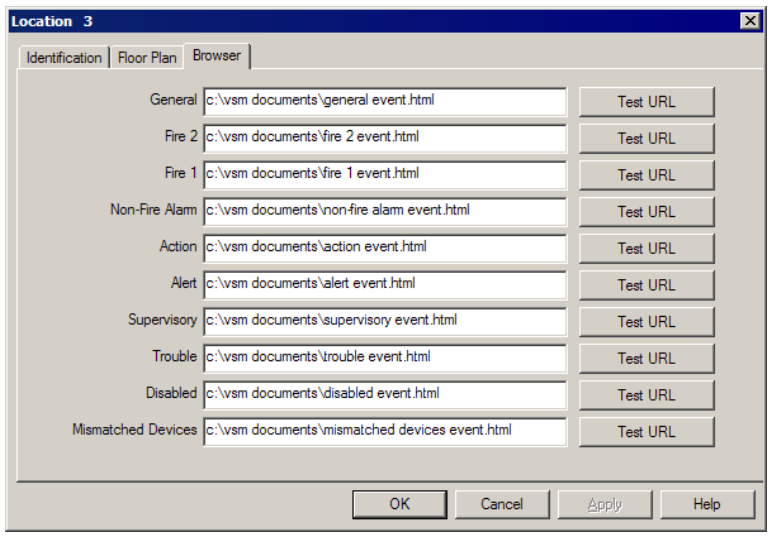


Figure 7-19: Edit Location: Document Event Type Assignment

7.6 Device Status View

The current status of a live device can be viewed in the Device Status view. This view only applies to live devices and will automatically close if the device drops offline or the connection is lost.

The Status view may appear in the detail pane on a Device view when the device is selected on the tree. Alternately, a floating Status view can be created by selecting **View > Status** (refer to Figure 7-20).

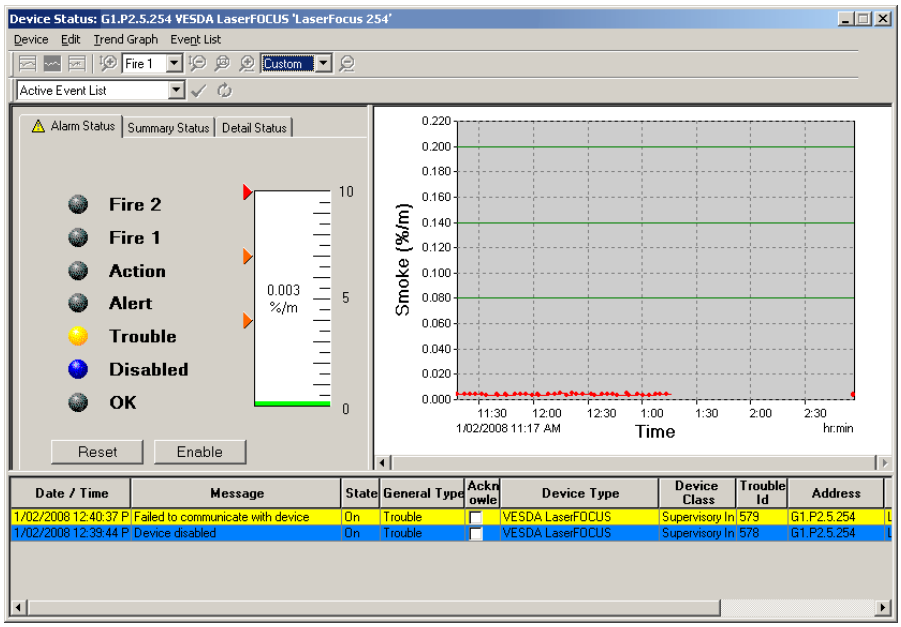


Figure 7-20: Status View (floating)

The status view combines a trend graph, an Active Event List and status pages that are all restricted to the selected device and any associated devices.

The Trend graph and Active Event List sub-views behave identically to the standard views (refer to sections 7.9 and 7.2) and have the same menus and toolbar buttons. The graph shows the variation in the measured value with time, so that trends can be readily observed. The Active Event List allows troubles and alarms directly associated with the device to be readily observed and acknowledged.

The Trend Graph tab of the Options dialog (Figure 7-21) sets the cache size for devices which determines the history that is immediately available to the Status View when the device is selected and the Status View shown. Increasing cache size will consume more RAM and so an estimate of this is shown on the dialog.

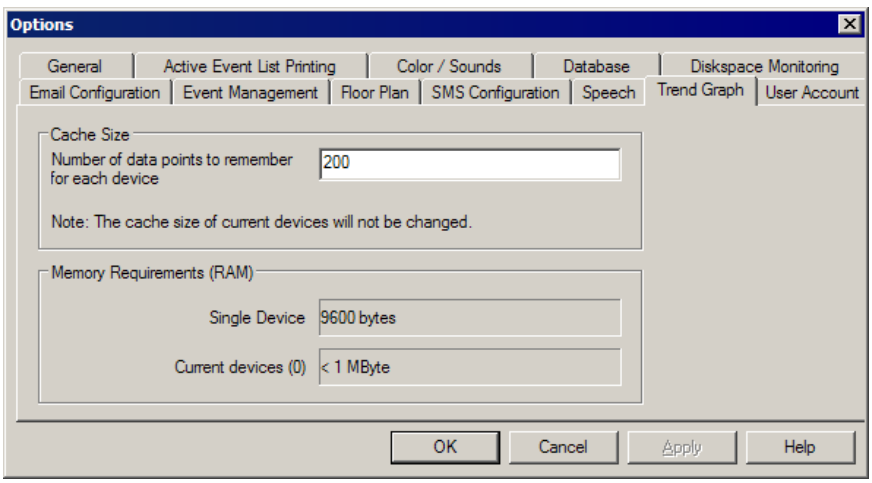


Figure 7-21: View > Options > Trend Graph

- **Cache Size -** Enter the number of data points for each device to remember. The cache size of current devices will not be changed until you disconnect and reconnect to the device.
- **Memory Requirements (RAM) -** The memory requirement calculations for the cache size are displayed. These fields are not editable.

7.6.1 Status Pages

The Status pages provide the following information:

- **Alarm status -** This tab applies only for detectors and contains primary information in graphic format, including a traffic light indicator which shows the event level, and a bar graph showing the current smoke level from an Xtralis VESDA detector (or temperature for a heat detector).
- **Summary status -** This tab contains primary information in text format, including alarm status, smoke level, current airflow and filter status.
- **Detail status -** This tab contains detailed status information in tabular format.
- **Associations -** This tab contains a list of devices that are associated with the original device, such as reference detectors or display units.

The Reference Detectors list shows other detectors that this device references. For example an Xtralis VESDA display may reference a detector, or one detector may reference the smoke level on another detector. The Dependant Devices list shows which other devices are referencing the current device.

Double-clicking on any device entry in either list will bring up the Device Status View for that device.

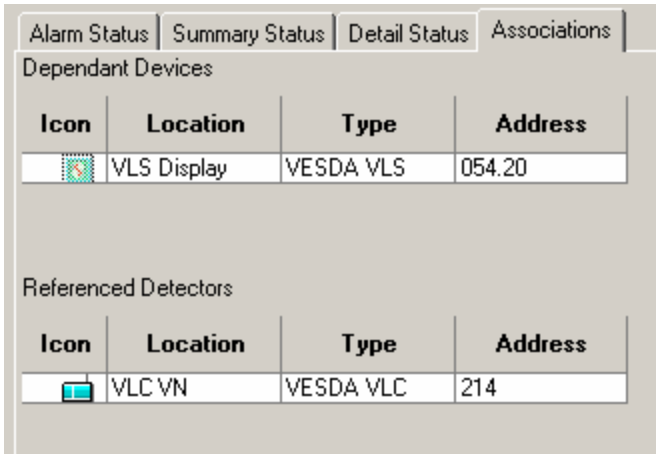


Figure 7-22: Image - Reference Tab

7.7 Monitor Browser

A Monitoring Site view provides a network-centric view of the system. The view itself is divided into two vertical panes: the navigation tree on the left and the area on the right showing a detailed view of the selected tree node. Usually, when containers or loops are selected on the tree a grid will be shown on the right which lists all its children. When a live device is selected in the tree then its Status View is shown on the right (refer to Section 7.6).

7.7.1 Constructing a New Monitoring Site

Building the monitored structure involves starting with a Monitoring Site (select **File > New > Monitoring Site**). Logical Nodes can then be inserted by selecting a tree node and using the Insert context menu (refer to Figure 7-23 below).

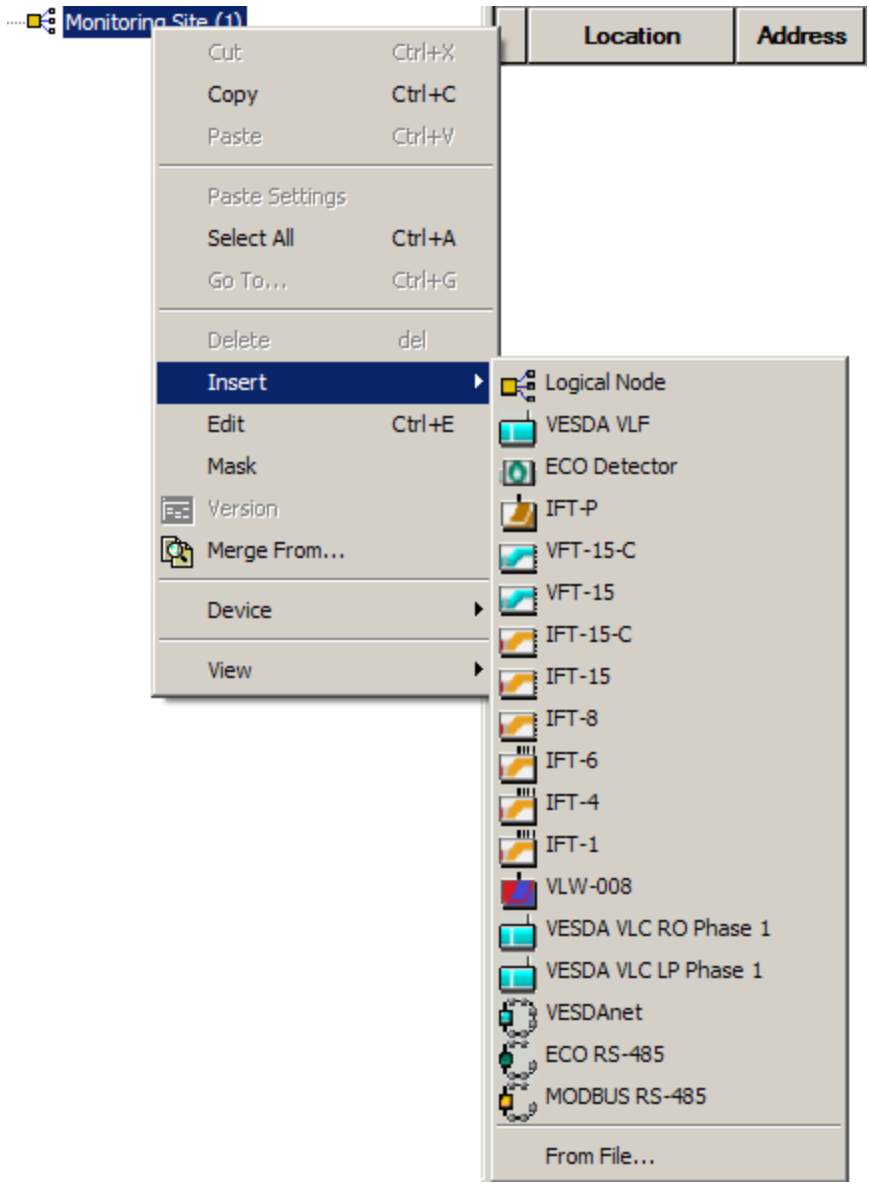


Figure 7-23: Insert Context Menu

As each node is inserted it should be edited to give it a meaningful name.

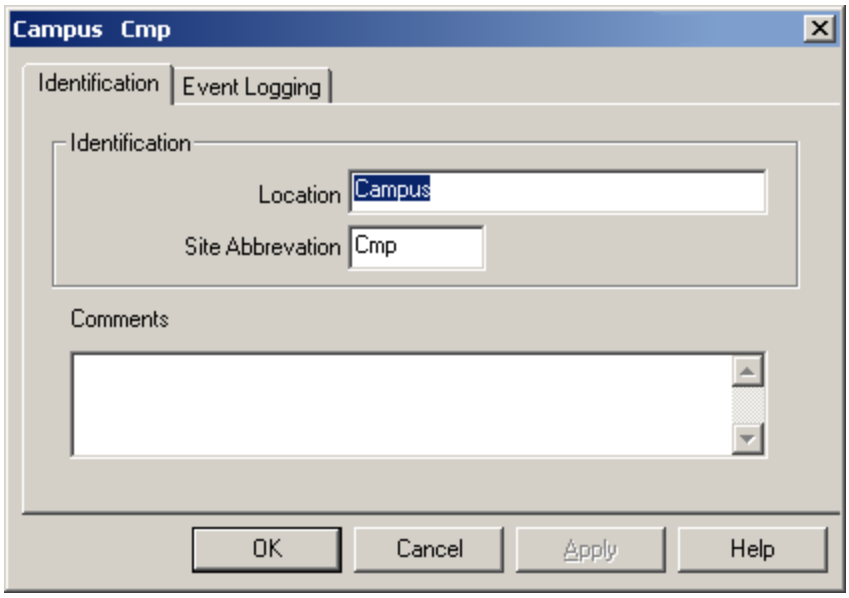


Figure 7-24: Diagram

At some stage the Designer attaches a network to the logical structure by inserting a VESDAnet (refer to Figure 7-25), followed by one or more detectors or other devices.

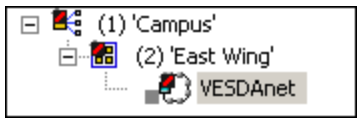


Figure 7-25: VESDAnet Insertion

The row representing the detector should be dragged in the grid to the actual address of the real detector or device.

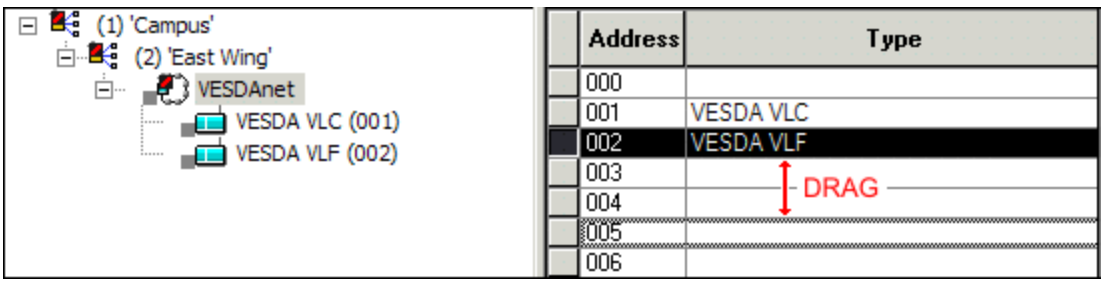


Figure 7-26: Assign Address

Once this has been done then the Designer should edit the VESDAnet connection properties. The Connection tab will allow the designer to define the connection that VSM4 will use to connect this item to the real devices. The Browse button on the dialog will bring up the Connection Manager which displays all defined connections and also provides wizards to guide the designer in defining new connections. These are described further in Appendix D.

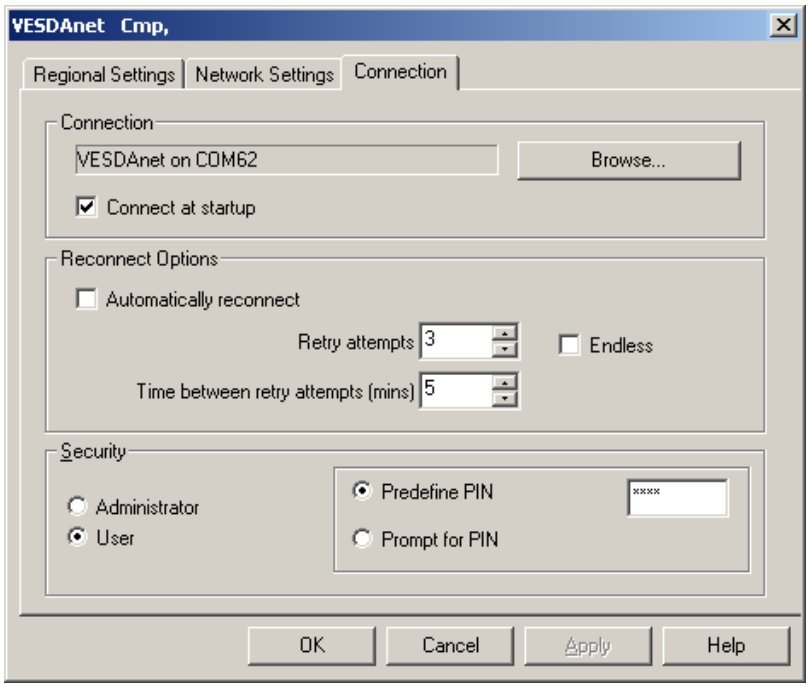


Figure 7-27: Connection Tab

The connection tab also allows the automatic reconnection rules to be defined and allows the Designer to predefine the specific access PINs for this VESDAnet. It is recommended that the Designer define all the PINs up to Administrator level.

Once the Connection has been defined then the Designer can click on the Connect and Synchronize toolbar button (if there is access to the real system) to connect and retrieve all the networked devices monitored by this VESDAnet.

Similarly, connections need to be defined for all the other networks that are to be monitored. Once this is done then the structure should be saved.

7.7.2 Menus

The menus update whenever the selection changes within the view. This may be as subtle as changing focus from a container on the tree to a child on the grid. The menus will show the commands and views that are relevant for the selected device. If the device has dropped offline then the commands will be hidden and the views will be restricted.

Context Menu

Most of the main Edit menu commands are available on the context menu. The device commands and view commands are supported as cascaded menus.

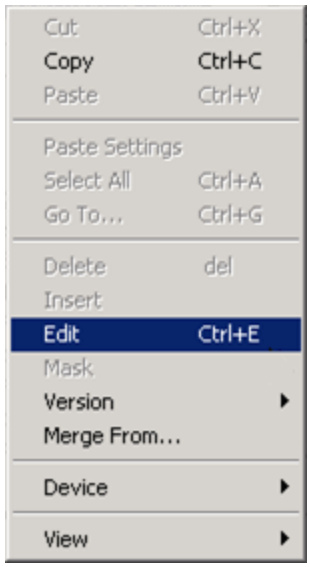


Figure 7-28: Context Menu

7.7.3 Editing Devices

Editing options vary depending on whether the device is live or offline and if live on the current access level. If a configuration is offline, such as when it is being worked on by the Designer, then all the devices may be edited or deleted. However, a live device can not be deleted as it makes no logical sense and hence it can not be 'cut' to the clipboard, although it can be copied to the clipboard.

The Edit command is always available for a device but if the operator is not logged on with Administrator access then they may view but not change the properties.

7.7.4 Grid Operations

Device addresses are set by the row that they occupy on the grid. Dragging them to another row changes their address. This can only be done if an operator is logged on at Administrator level. Multiple devices may be moved at the same time by doing a multiple selection and then dragging them. They will then be placed consecutively at the new starting address in the same order.

When selecting devices, the Shift key defines a continuous range from the first selected device and the Ctrl key toggles the selection of the single row that is clicked on.

7.7.5 Cell Editing

Individual cells on the grid may be edited (as long as they don't represent read-only properties) by switching to cell editing mode using **Device View > Cell Editing**.

In this mode clicking in a cell will allow the user to directly edit the text, or drop down a list of possible values as a combo box. The user needs to be logged on with Administrator access to be able to do this. The tab, back-tab keys can be used to move between fields. Cells can be copied and pasted to other tools (such as spreadsheets) and cell text from spreadsheets may be pasted into grid cells. While working in cell editing mode the context (and main Edit) menu will refer to cell operations. For example, the clipboard operations (Cut, Copy, Paste) will be in terms of the text in the cells. Drag and drop will also move individual cells, not devices.

To select a row, while in cell editing mode, click on the button to the left of the row.

Figure 7-29: Select Row

Selecting a row also changes the context menu to refer to the device represented by that row.

7.7.6 Viewing Devices

Each node in the tree comprises two icons. The main icon represents the device type with an overlay. The icon to the left of the device icon represents the state of the device. The icons are listed below.

Table 7-1: Monitoring Structure Icons

Icon	Description
	Trouble
	Device is offline
	Alert on device with one fire level
	Action on device with only one fire level
	Alert on device with both Fire 1 and Fire 2
	Action on device with both Fire 1 and Fire 2
	Fire1 on detector
	Fire 2 on detector
	Device is in Loader mode
	Gas Alarm
	Gas Pre-Alarm

Overlay	Description
	Device icon with no overlay
	Device has changed since it was last saved or last synchronized with the live device.
	The device is running a command
	The device has been found but no configuration is yet available
	Device is disabled

Tree Node Customization

The text shown for the tree nodes can be customized by editing its template using the **Device View > Customize Tree** menu item. The Device View shares the same template. The details of editing the template are described in section 7.4.15.

7.7.7 Splitting the View

Multiple Monitor Browser views can be opened on the same model by clicking on one view and then selecting **View > Monitor Browser** (when logged on as Designer). These views are all synchronized so that edits made on one will appear on the other. This can be useful to allow two different loops to be edited at the same time or to allow devices to be copied from a grid in one view to a grid of another loop in a second view.

7.8 Device View

The device view is a restricted form of the Monitoring Browser that does not support logical nodes so that it can only be associated with a single network connection.

7.8.1 Printing

File > Print and **File > Print Preview** will print configuration details of the device selected in the tree and all its descendents. To print details on a single device, select it and then invoke Print. To print the entire system, select the root node in the tree, and then invoke Print.

7.9 Trend Graph

The time variation of the detector's measured values can be shown on the Trend graph. As the name suggests this allows trends in the readings to be visually separated from noise. For pre-alarms this could distinguish between a slow buildup of smoke causing an Alert threshold to be tripped or a threshold that has been set too low and is in the signal noise. The Trend graph allows multiple devices to be plotted so that their readings can be visually compared.

Open a Trend Graph

Select an icon or region that represents a detector and then invoke **View > Trend Graph** from its context menu to graph the detector. The operator is prompted with a filter window (see below) where they can choose to plot historical and/or live measurements:

- **Live -** Displays readings as the data is received
- **Historical -** Displays readings from the database or the device's event log. The plotted events can be restricted to a specific time and date range.

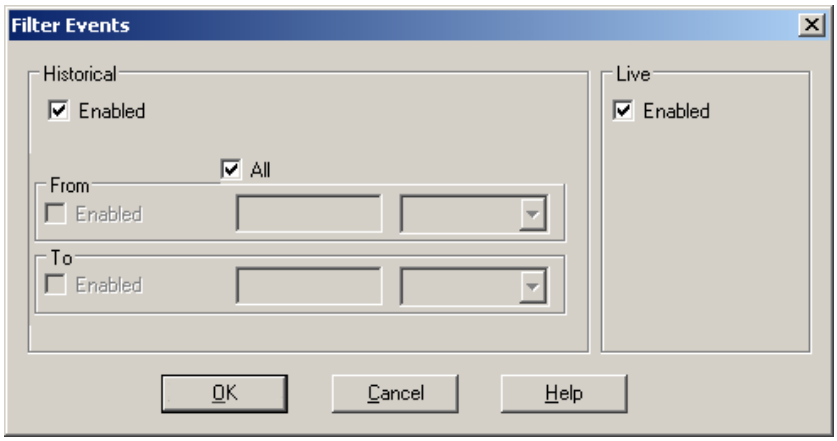


Table 7-2: Filter Dialog

After making a selection, a new graph view is opened, unless one is already open for the current connection. If a trend graph is already open then the detector is added.

Additional devices can be added by repeating the above steps or by drag and dropping them onto the graph. For example, multiple devices can be selected in a grid and dragged and dropped onto a graph.

Note: Graphs will currently only accept devices sharing the same connection since the graph uses the network time (associated with the connection) for its time axis.

7.9.1 Elements

A trend graph can contain multiple sub-graphs as shown below, when devices that measure different quantities are plotted against each other. Each sub-graph is associated with a specific quantity. For example, in the graph below, the top sub-graph shows outputs from two devices in raw units and the lower sub-graph shows smoke measurements. All sub-graphs share the same time scale and so scroll together.

The legend appears to the right of each sub-graph. It lists the devices that are plotted and allows commands on these devices to be invoked by using a context menu.

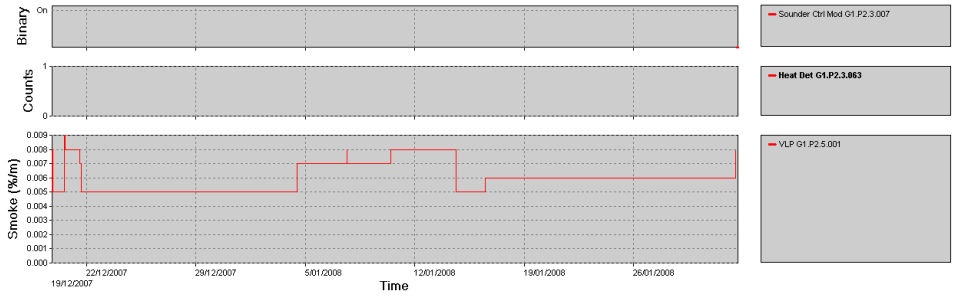


Figure 7-30: Trend Graph

7.9.2 Legend

The legend defines the color for each plotted device and identifies the detector by abbreviation and address. Detectors with multiple inputs such as the VLS show a line for each input sector.

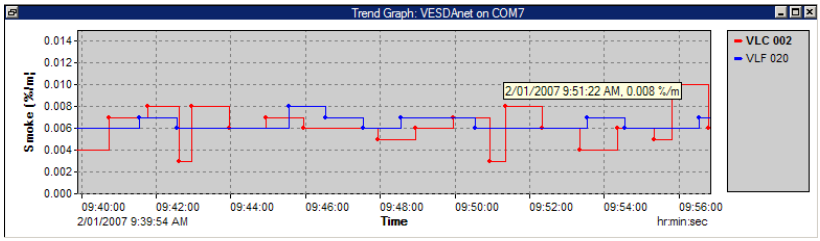


Figure 7-31: Trend Graph View with Legend

When multiple devices are plotted one is defined as the 'current' device and is shown bolded in the legend. The current device defines the threshold levels which are shown on the graph and which are used to define the Fire1 and Fire2 vertical scales.

7.9.3 Hiding / Showing Device

Right-clicking on a device entry in the legend will bring up a context menu which allows devices to be hidden or shown on the graph. Hidden devices are shown as greyed-out entries on the legend. The context menu provides access to commands and views that are relevant to the device.

7.9.4 Removing Device

Right-click on the device entry in the legend in the legend and invoke Delete from the context menu. Alternatively, left-click on the device entry in the legend and hit the **Delete** key.

7.9.5 Display

- **Thresholds -** Green horizontal lines indicate the thresholds for the currently selected device (e.g. Fire 1, Fire 2). To identify a threshold line and see its exact value, position the mouse pointer over it and read the tooltip, as shown below. Some of the more sophisticated detectors have separate threshold banks for day and night operation and will automatically swap between these banks. The operator can choose to show the Day, Night or Current thresholds on the graph by clicking on the relevant button on the graph toolbar.

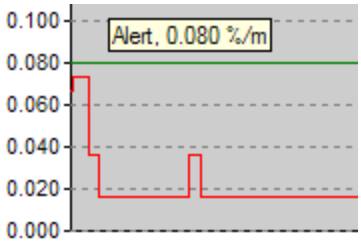


Figure 7-32: Tooltip showing the name and value of the threshold level

- **Data Points -** Points where the measured reading changed are shown as round dots if the graph is zoomed in sufficiently. As the graph is zoomed out the dots disappear and only the line remains, as shown above. Points where readings ceased or restarted, due for example to the loss of power, are shown as breaks in the graph.
- **Tool Tips -** Positioning the mouse pointer over change points along the line will show a tooltip giving the exact date, time and value for that point.

7.9.6 Navigation

The graph allows the user to zoom and pan through the data to locate and view relevant data.

Zoom

Toolbar buttons and menu commands are provided for the zoom as detailed below. The zoom can also be specified by clicking on a graph and dragging out a rectangular region of interest. The graph will scale to this region. If the shift key is held down while dragging out the region then only the time range will be affected; the vertical range will remain the same.

Pan

The horizontal and vertical scrollbars are used to pan the view. The vertical scroll bar will not be shown if all the data points are already within the vertical range of the graph.

- **Live Setting -** The Trend Graph display will track live data if the graph is scrolled to include the current time by scrolling the horizontal scroll bar to the extreme right. When this is done the right arrow at the end of the scroll bar is disabled. If the scroll bar is moved to the left, or the user zooms in on data at an earlier time, then the graph display will stay locked on the specified time range and the scroll bar will move to the left as the displayed time falls further behind the current time.

Resize

As the graph view is shrunk the information around the graph will be minimized so that the graph itself stays visible. First the scale labels are reduced and then the axis labels will be removed and eventually only the line graphs will remain.

The legend usually scales with the graph window. The legend size can be independently varied by clicking with the mouse in the gap separating the sub-graph and legend and dragging the separator to the desired width.

Export

Data can be exported to other applications via the clipboard or by saving to a csv file.

- **Copy/paste graph image -** Select the Trend Graph and press Ctrl+C to place a copy of the Trend Graph image into the Windows clipboard.
- **Export as csv file -** The graph data can be exported as a Comma Separated Value (csv) file by selecting **File > Save** which can then be imported into Excel. However, VSM4 will not open and load this file.

Print

To print a graph, select **File > Print**.

Toolbar and Menu

The Trend Graph Toolbar is shown below:

Figure 7-33: Trend Graph Toolbar

- The first three buttons act as radio buttons to specify the thresholds. They specify the day, night and current detector thresholds, respectively.
- The vertical magnification buttons specify the vertical zoom in, special zoom and zoom out.
- The special zoom dropdown lets the range be set to standard pre-defined values as shown below. The Fire1 and Fire2 ranges are based on the levels for the device that is currently selected (shown in bold) on the legend.

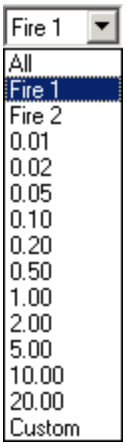


Figure 7-34: Special Zoom

- The Show All button will set the horizontal and vertical ranges to cover all the data points.
- The horizontal magnification buttons specify the horizontal zoom in, special zoom and zoom out.
- The Menu lists the functions of the toolbar except for the special zoom options.

7.9.7 Options

The Trend Graph tab of the Options dialog contains the settings used to specify the size of graph data caches that are held by devices. It is the data in these caches that is plotted when a Device Status view is displayed.

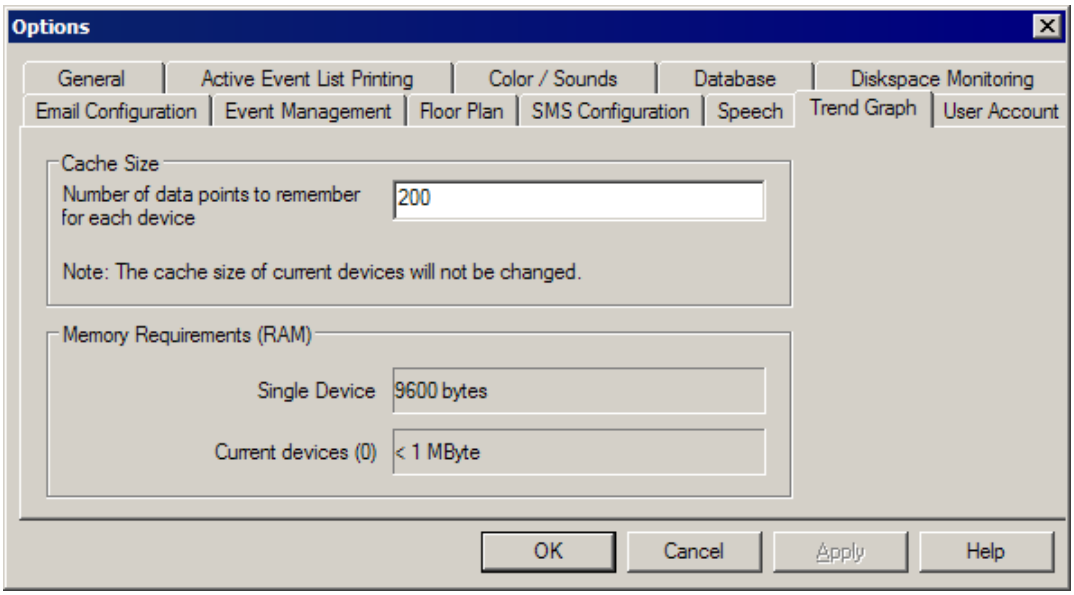


Figure 7-35: Trend Graph Options

Trend Graph Settings

- **Cache Size -** Enter the number of data points that each device caches. Changes to this setting only take effect after disconnecting and then reconnecting to the network.
- **Memory Requirements (RAM) -** The memory requirement calculations for the cache size are displayed. This field is not editable.

7.10 Event Log View

Event Logs of state changes and user actions are maintained within Xtralis VESDA detectors. VSM4 should be setup by the Designer (refer to Chapter 3) to integrate these logs into a database.

The Event Log View displays these historical events. It can be used by an administrator to verify correct system operation, fine-tune system settings or to troubleshoot equipment faults. Event data may be loaded from a file, retrieved from a detector or obtained from a database. Either way it is viewed on an Event Log View.

Open Event Log View

Select **View > View Database Events** or click on the Event Log view button on the main toolbar to open a view of the events.

Before the Event Log is opened, the Filter Events dialog is displayed. For example, Figure 7-36 below shows the filter for the database.

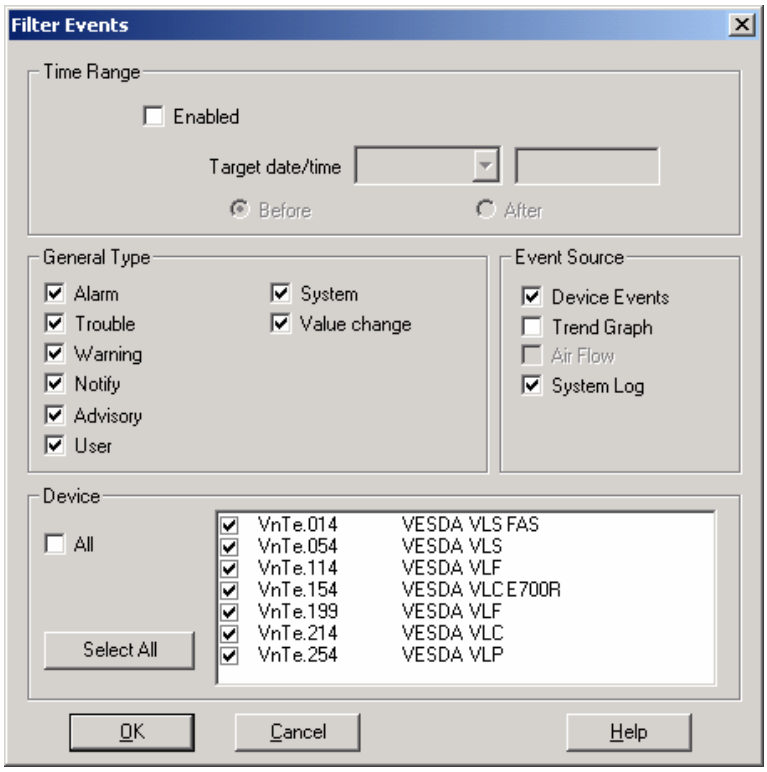


Figure 7-36: Filter Events

The panels on the filter allow the user to define:

- When the events occurred (i.e. the relevant time range). A starting date/time or a finishing date/time can be defined.
- The relevant event types.
- The source of the events, for example device events, trend data or system events. The system events show who is logged onto VSM4 and so can be used to associate an operator with an action.
- Where the events occurred, i.e. which devices to collect events for.

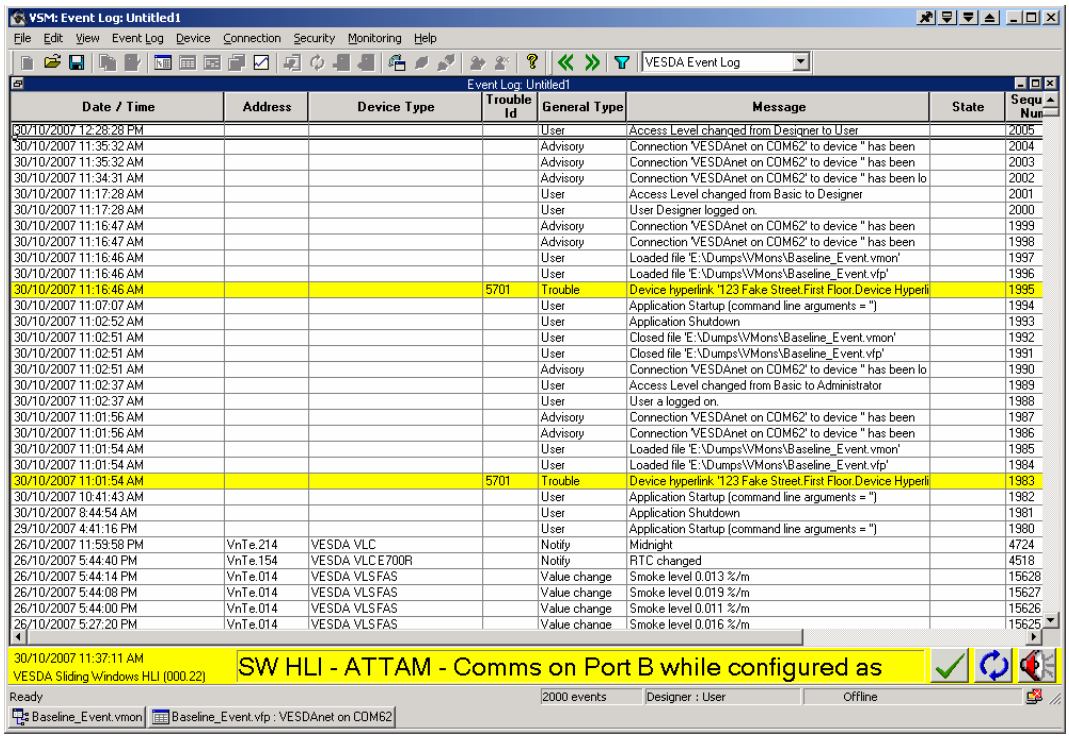

VSM: Event Log: Untitled1
File Edit View Event Log Device Connection Security Monitoring Help
VESDA Event Log
Event Log: Untitled1
Date / Time | Address | Device Type | Trouble Id | General Type | Message | State | Sequ Num
30/10/2007 12:28:28 PM | | | | User | Access Level changed from Designer to User | | 2005
30/10/2007 11:35:32 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been | | 2004
30/10/2007 11:35:32 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been | | 2003
30/10/2007 11:34:31 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been lo | | 2002
30/10/2007 11:17:28 AM | | | | User | Access Level changed from Basic to Designer | | 2001
30/10/2007 11:17:28 AM | | | | User | User Designer logged on. | | 2000
30/10/2007 11:16:47 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been | | 1999
30/10/2007 11:16:47 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been | | 1998
30/10/2007 11:16:46 AM | | | | User | Loaded file 'E:\Dumps\VMons\Baseline_Event.vmon' | | 1997
30/10/2007 11:16:46 AM | | | | User | Loaded file 'E:\Dumps\VMons\Baseline_Event.vfp' | | 1996
30/10/2007 11:16:46 AM | | | 5701 | Trouble | Device hyperlink '123 Fake Street.First Floor.Device Hyperli | | 1995
30/10/2007 11:07:07 AM | | | | User | Application Startup (command line arguments = '') | | 1994
30/10/2007 11:02:52 AM | | | | User | Application Shutdown | | 1993
30/10/2007 11:02:51 AM | | | | User | Closed file 'E:\Dumps\VMons\Baseline_Event.vmon' | | 1992
30/10/2007 11:02:51 AM | | | | User | Closed file 'E:\Dumps\VMons\Baseline_Event.vfp' | | 1991
30/10/2007 11:02:51 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been lo | | 1990
30/10/2007 11:02:37 AM | | | | User | Access Level changed from Basic to Administrator | | 1989
30/10/2007 11:02:37 AM | | | | User | User a logged on. | | 1988
30/10/2007 11:01:56 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been | | 1987
30/10/2007 11:01:56 AM | | | | Advisory | Connection 'VESDAnet on COM62' to device '' has been | | 1986
30/10/2007 11:01:54 AM | | | | User | Loaded file 'E:\Dumps\VMons\Baseline_Event.vmon' | | 1985
30/10/2007 11:01:54 AM | | | | User | Loaded file 'E:\Dumps\VMons\Baseline_Event.vfp' | | 1984
30/10/2007 11:01:54 AM | | | 5701 | Trouble | Device hyperlink '123 Fake Street.First Floor.Device Hyperli | | 1983
30/10/2007 10:41:43 AM | | | | User | Application Startup (command line arguments = '') | | 1982
30/10/2007 8:44:54 AM | | | | User | Application Shutdown | | 1981
29/10/2007 4:41:16 PM | | | | User | Application Startup (command line arguments = '') | | 1980
26/10/2007 11:59:58 PM | VnTe.214 | VESDA VLC | | Notify | Midnight | | 4724
26/10/2007 5:44:40 PM | VnTe.154 | VESDA VLC E700R | | Notify | RTC changed | | 4518
26/10/2007 5:44:14 PM | VnTe.014 | VESDA VLS FAS | | Value change | Smoke level 0.013 %/m | | 15628
26/10/2007 5:44:08 PM | VnTe.014 | VESDA VLS FAS | | Value change | Smoke level 0.019 %/m | | 15627
26/10/2007 5:44:00 PM | VnTe.014 | VESDA VLS FAS | | Value change | Smoke level 0.011 %/m | | 15626
26/10/2007 5:27:20 PM | VnTe.014 | VESDA VLS FAS | | Value change | Smoke level 0.016 %/m | | 15625
30/10/2007 11:37:11 AM
VESDA Sliding Windows HLI (000.22)
SW HLI - ATTAM - Comms on Port B while configured as
Ready
2000 events
Designer : User
Offline
Baseline_Event.vmon
Baseline_Event.vfp : VESDAnet on COM62

Figure 7-37: Event Log for detectors on a VESDAnet

7.10.1 Event Retrieval

Once the data has been retrieved the number of events is shown in a panel below the status bar. Page forward/backward buttons are provided on the toolbar to request further events going backwards from the end or forwards from the start of the displayed events. The maximum number of viewed events is 20,000. Once this limit has been reached paging forwards to further events will cull the oldest events. Similarly paging backward will cull the earliest events.

The filter toolbar button allows the displayed data to be further filtered. It brings up the Filter Events dialog shown above. If the filter conditions are made more restrictive, then the filtering is done in RAM and is fast. If the filter conditions are relaxed beyond the conditions associated with the original database retrieve then the data will be fetched again from the database which is slower.

The Event Log menu provides access to the Grid Style Manager as well as these event retrieval and filtering commands.

7.10.2 Display Controls

The Event Log table style can be changed to one of the pre-defined ones by using the table style selector on the toolbar (see below). Additional table styles can be created using the Grid Style Manager (refer to section 7.2.6).

The Event Log table can be sorted by column. This is done by clicking on the heading of the desired column. This will sort in ascending order. Clicking again will toggle it to sort in descending order.

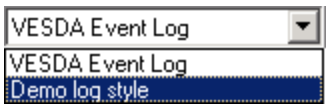


Figure 7-38: Table Style Selector

The event counter in the status bar shows how many events are displayed in the table (Figure 7-39).

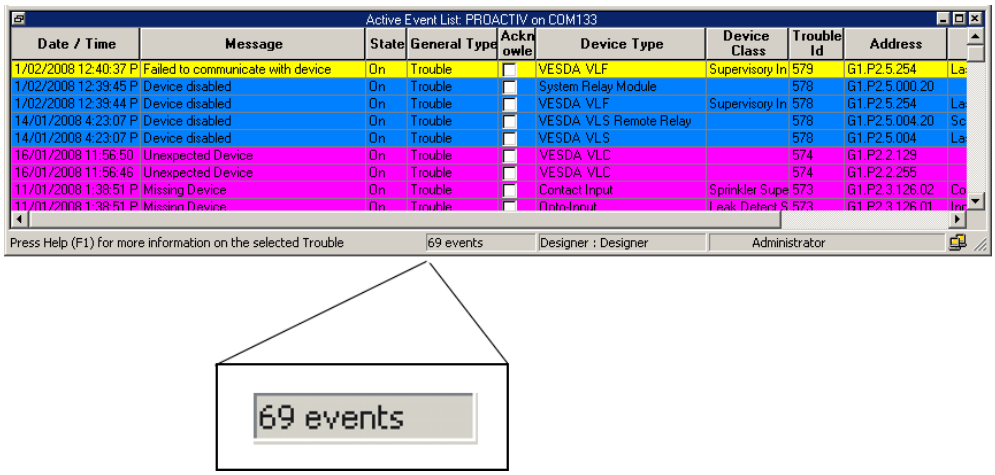

Active Event List: PROACTIV on COM133
Date / Time
Message
State
General Type
Acknowle
Device Type
Device Class
Trouble Id
Address
1/02/2008 12:40:37 P Failed to communicate with device On Trouble VESDA VLF Supervisory In 579 G1.P2.5.254
1/02/2008 12:39:45 P Device disabled On Trouble System Relay Module 578 G1.P2.5.000.20
1/02/2008 12:39:44 P Device disabled On Trouble VESDA VLF Supervisory In 578 G1.P2.5.254
14/01/2008 4:23:07 P Device disabled On Trouble VESDA VLS Remote Relay 578 G1.P2.5.004.20
14/01/2008 4:23:07 P Device disabled On Trouble VESDA VLS 578 G1.P2.5.004
16/01/2008 11:56:50 Unexpected Device On Trouble VESDA VLC 574 G1.P2.2.129
16/01/2008 11:56:46 Unexpected Device On Trouble VESDA VLC 574 G1.P2.2.255
11/01/2008 1:38:51 P Missing Device On Trouble Contact Input Sprinkler Supe 573 G1.P2.3.126.02
Press Help (F1) for more information on the selected Trouble
69 events
Designer : Designer
Administrator
69 events

Figure 7-39: Event Counter

7.10.3 Save / Load

Event logs can be saved in binary file (i.e. in .vevt format) by selecting **File > Save As**.

These files can be reloaded into VSM4 by selecting **File > Open** and are language neutral.

7.10.4 Export

Event logs can be exported to a text file by selecting the **File > Save As** menu item. The data in the columns is saved as tab separated text. Such files can be loaded into spreadsheets for further analysis. Note that VSM4 is unable to load these files.

The contents of the Event Log table can be copied to the Windows clipboard. To achieve this, select a range of events in the list, then press **CTRL+C**. The copied data is formatted using tab delimiters in-between columns. The column headings are automatically included in the exported data.

7.10.5 Printing

The **File > Print** (and Print Preview) commands allow an event log to be printed out. Where the printed table exceeds a single page, column headings are repeated on each page.

7.10.6 Plotting

Event data can be trended using the Trend Graph (select **View > Trend Graph**). This option will only be available if the log contains value change events.

8 Workspace Configuration

The management of multiple views is described in this section. These views can be positioned across multiple displays.

8.1 Display Structure

VSM4 uses the display concepts illustrated below (Figure 8-1). The VSM4 application manages frames which usually correspond to the physical screens associated with the workstation. Views are then placed within partitions on a frame.

We first look at how views are managed within a frame and then proceed to discuss the support that VSM4 has for multiple frames and through that for multiple screens.

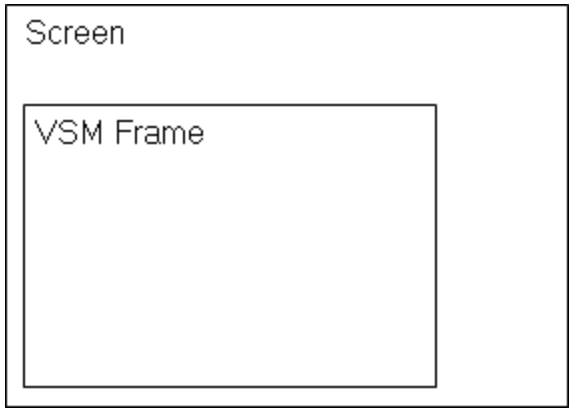


Figure 8-1: Display Structure

8.2 View Management

Views are normally placed in a partition on the active frame so that they won't be lost or hidden behind other views. Each new view that is opened causes the frame to add a new partition which shrinks the existing views to make room for the new view. The balance between the partitions can be adjusted by moving the splitter.

At the top of each view is a title bar and the standard minimize, maximize and close buttons.

- The title bar indicates the type of view and the file and connection (where relevant) that the view is associated with.
- The minimize control will remove the partition and place a button in the application status band underneath the Status Bar. Clicking on the button will cause the view to be restored as the lowest partition.
- The maximize control causes all other views to be minimized so that the current view takes up the entire frame.
- The Close control completely removes this view.

8.2.1 Current View

When the user clicks somewhere on a view, it becomes 'current'. The title bar of the view changes and its title is placed in the application's title bar. Also the menus and toolbars associated with the current view are integrated in with the main menus and toolbars.

The user can cycle between the views by pressing **F6**. **F5** can be used to cycle between elements in the same view, such as between the tree and grid in the Monitoring Structure.

8.3 Multiple Displays

Support for multiple display screens is achieved by providing secondary frames. Secondary frames are similar to the primary frame, except that they don't contain the status bar. They can be freely positioned and sized, and contain views just like the primary frame. As an example, the Floor Plan view and Status Bar can be positioned on one screen and all other views on another frame that is positioned on a second screen.

When the software is launched, the application opens a single frame, with a menu and toolbar. At this point it is possible to maximize, minimize or resize the frame, or move it to another screen.

Button	Description
	Detach Frame.
	Select Target Frame.
	Minimize all but the current Frame. This control allows the user to minimize all frame windows except the one in which this control is activated.
	Minimize all Frames. This control allows the user to minimize all frame windows.
	Maximize all Frames. This control allows the user to maximize all frame windows.

Table 8-1: Frame Management Controls

In order to use multiple displays it is first necessary to open a view within the main frame, for example, a Floor Plan or a Monitoring Structure. The view can then be detached from its frame by clicking on the Detach button at the top left of the view's title bar. A secondary frame will open up containing the view. The new frame can be repositioned and resized as required. For example, it could be moved to another screen.

Once multiple frames exist, views can be dragged between them by clicking on their title-bars and dragging and dropping them onto the title bar of the destination frame. The view will be placed in the bottom partition of the frame that they are dropped onto.

Minimizing views will cause them to shrink to a button at the base of their frame the same as for a single frame system.

8.3.1 New Views

Any new views will be opened within the active frame. It is possible to over-ride this by activating target mode on any of the secondary frames. This is done by clicking on the pin control, located in the title bar next to the windows resizing controls. The pin changes to a target. In this mode, all new views will appear in this frame. To deactivate, left-click the control again to return to the default behavior, or click the pin control in another frame to select it as the target for new views.

8.4 Automatic Frame Behaviour

Whenever the highest priority event within VSM4 changes, then VSM4 maximizes the primary frame and places it on top of any other open window, so that the Status Bar is visible. This occurs even if the main frame has been minimized.

Secondary frames will remain minimized. However, if the secondary frames are visible then they also will be placed above all other windows when the highest priority event changes.

Closing a secondary frame closes the views it contains. Closing the primary frame closes the application and so also closes any secondary frames.

Note: The user must be logged on with Administrator level to close the application once a monitoring site has been opened.

This page is intentionally left blank.

A Prerequisites

A.1 Monitoring Computer

In order to install and run VSM4, the Monitoring Computer must conform to the minimum requirements, as listed below:

Item	Detail
Operating System	Microsoft Windows 2000, Windows XP, Windows Vista® or Windows 7
Processor	Pentium 4 2.8 GHz; 1 MB cache
Memory	2GB
Hard Disk	**Preferred:** 2 x 80GB connected to RAID Storage **Minimum:** 1 x 80GB
Display	**Preferred:** Two 19" SVGA screens, 1280x1024 **Minimum:** Single 19" SVGA screen, 1024x768
Display Adaptor	**Preferred:** Dual Monitor card with 256 MB memory **Minimum:** Single Monitor card with 128 MB memory
Network Adaptor	**Wired:** 100Mb/sec ethernet or greater **Wireless:** 54Mb/sec ethernet or greater
Serial Port	High Speed FIFO (16550 or compatible)
Audio	Sound output capability and speakers
Peripherals	DVD-ROM drive Line Printer (events) *Optional Printer (other) *Optional
Archiving	Writable DVD
Redundancy	Redundant Power Supply and Fans UPS
Database	If not using a VSM Managed or SQLite database, an ODBC-compliant database to store event and system logs. The database can be accessed either locally or remotely using a Windows data source.
Internet Connection	The following items require internet connection: • **Licensing:** web-based activation, during the licensing process. Where this is not available, activation can be done by phone. • **Updates:** obtaining of new software releases • **Notifications:** access to a remote email server or SMTP to SMS gateway
Web Browser	The following items require a web browser such as Microsoft Internet Explorer: • web-based license requests • display event response procedure documents

Table A-1: Minimum Monitoring Computer Requirements

Note: If other applications are to be used on the same system, the processor, memory and hard disk specifications may need to be increased. The extent of the increase depends on the aggregate resource requirements of all applications, and whether the applications need to be run concurrently.

A.2 Network Capacity

The performance of VSM4 may be affected by the performance of the network and the performance of network elements, such as the Serial-to-Ethernet Devices. S2E Devices are also known as serial port emulators.

A.2.1 Latency

Latency (or 'delay') is a critical performance parameter of a network used to support VSM4. For best performance, a network with good end-to-end response times is desirable.

A default connection timeout feature within VSM4 allows delays of up to 2 seconds. This is usually considered generous for most WAN applications. If the link is particularly slow, it is possible to increase the timeout period.

Refer to the Help system for further information on setting timeout periods.

A.2.2 Bandwidth

In a steady (no alarm / no fault) state, each connection will consume approximately 0.1 Kbit/s.

The maximum bandwidth is consumed during the initial establishment of a connection between the VSM4 software and the connecting device. Under this circumstance, each connection could consume approximately 8Kbit/s.

A complete VLP event log, when framed for transmission, represents only approximately 100KBytes. Throughput by the detector will vary, depending on its other responsibilities at any given time, but will not exceed 16Kbits/s.

A.2.3 Load

The load on VSM4 is directly related to the number of devices (mainly detectors) that it is monitoring. There is an additional but minor impact for each network connection.

B Checklists

B.1 Planning Checklist

The following material should be assembled for handover to a designer:

☐	Licensing – A license should be purchased with sufficient capacity (refer to section 2.2.5) to cover all monitored devices. A Site License number was provided at the time of purchase. This is required for product activation.
☐	IT Planning Checklist completed (see following sheet)
☐	Photos for each campus or building
☐	Floor plans for each level of each building with locations of detectors and fire zones marked up. Network connections should be specified.
☐	Text to Speech: Messages to be spoken when an alarm or trouble occur
☐	HTML Browser: Alarm response procedure documents. If provided then such documents can be automatically displayed when alarms occur on floor plans. Targeted documents that apply to specific areas can be included. These may contain details on dangerous chemicals or special evacuation procedures.
☐	List of operators and their required access levels (e.g. User or Administrator access).
☐	Remote Notification: List of users to be notified remotely. The users need to be listed according to work shifts and their email addresses should be included. The information and format of the sent emails should be specified.

B.2 IT Checklist

The site should tick which features are relevant and then get their IT department to complete the relevant sections.

Feature	IT Responsibility
☐ External access required	☐ Has firewall been updated? ☐ NAT used External IP address: _____ . _____ . _____ . _____
☐ Using (MOXA) serial to IP converters Number of MOXAs	☐ MOXA serial to IP Converters require access to the following ports: • TCP 950-981 • UDP 1029 • TCP 4000 • TCP 4900 • UDP 4800 MOXA IP addresses. Each MOXA requires an IP address: Moxa 1: _____ . _____ . _____ . _____ Moxa 2: _____ . _____ . _____ . _____ Moxa 3: _____ . _____ . _____ . _____ Moxa 4: _____ . _____ . _____ . _____ ☐ Do MOXAs cross firewall? If the MOXAs cross the firewall then the ports listed above will need to be accessible across the firewall. ☐ NAT used
☐ Remote Notification	Email Server : _____ VSM4 email address: _____ ☐ SSL required The following are only required if the server requires user logon. User Account: _____ Password: _____

Feature	IT Responsibility
☐ Database Number of secondary PCs: ____	**Primary Database** Shared Drive: _____ Database type (select one) ☐ VSM Managed ☐ SQLite ☐ Other ODBC (Specify) _____ ☐ Login required User Account: _____ Password : _____ Database Backup planned every ☐ Day ☐ Week on (day) ☐ Other (specify)
	Secondary Database 1 Shared Drive: _____ Database type (select one) ☐ VSM Managed ☐ SQLite ☐ Other ODBC (Specify) _____ ☐ Login required User Account: _____ Password : _____ Database Backup planned every ☐ Day ☐ Week on (day) ☐ Other (specify)

Feature	IT Responsibility
	Secondary Database 2 Shared Drive: _____ Database type (select one) ☐ VSM Managed ☐ SQLite ☐ Other ODBC (Specify) _____ ☐ Login required User Account: _____ Password : _____ Database Backup planned every ☐ Day ☐ Week on (day) ☐ Other (specify)

C Serial to Ethernet Connection

This Appendix of the VSM4 Product Guide provides information on the configuration of a MOXA Nport Server for use in Serial to Ethernet protocol conversion.

RS232/485 serial communications from a High Level Interface (HLI), a compatible detector or an IFT/VFT RS485 Modbus network may be connected to one side of a Serial to Ethernet Device, and a 10/100 Mbps Ethernet connection on the other side then provides connectivity to the devices over a TCP/IP network.

Depending on the selected configuration, any computer with IP connectivity and running VSM4 is able to establish communications with a High Level Inferface (HLI) or compatible detector. Locations where Serial to Ethernet would be useful include:

- Large site and campus site monitoring
- Remote site management and maintenance
- Campus integration
- Unmanned or inaccessible sites

C.1 Example Configuration

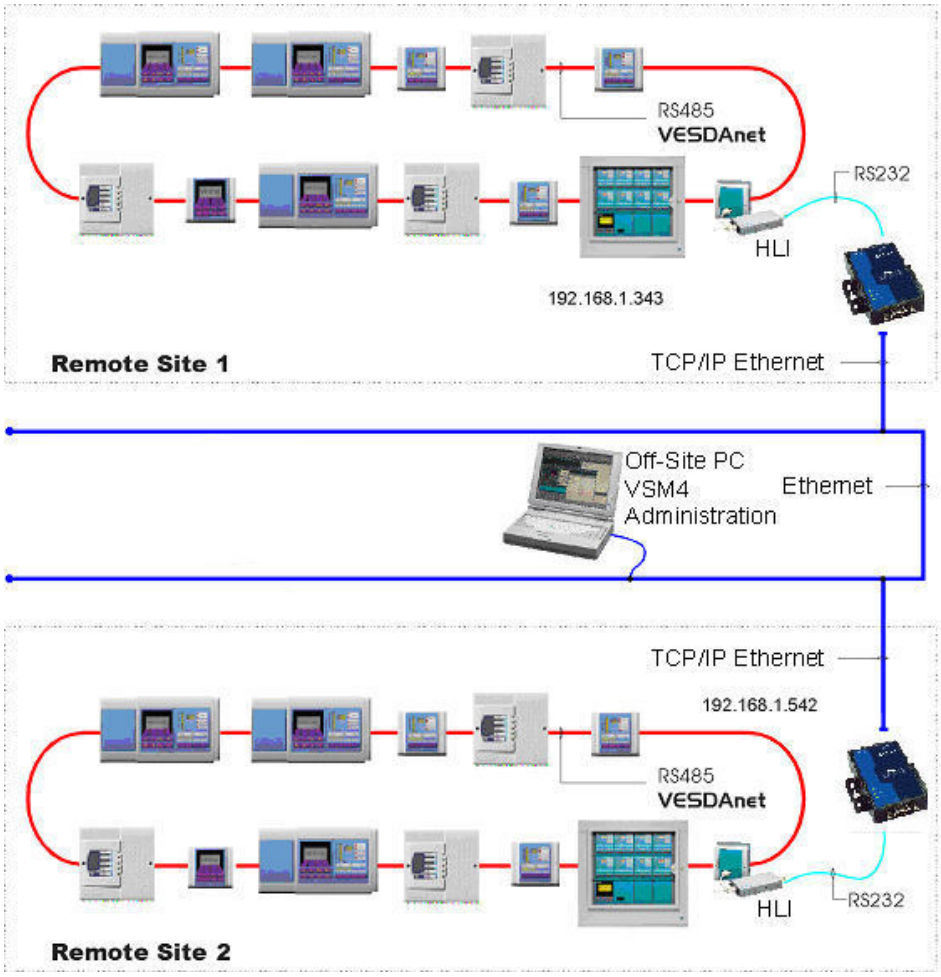


Figure C-1: Example Configuration

- The Monitoring Computer is connected to the High Level Interface (HLI) via a Serial to Ethernet device.
- Each Ethernet device is assigned an IP address.
- Software for configuring the Serial to Ethernet device is installed on the Monitoring Computer and various parameters are set, creating virtual COM port(s).

- Windows recognizes the virtual port on the Serial to Ethernet device as a real COM port.
- It is possible to connect a PC to a Serial to Ethernet device located outside the PC's LAN. This requires information about the public IP and Gateway addresses associated with the Ethernet device. Consult with your IT Administrator regarding connectivity options between your PC and the Serial to Ethernet device.

C.2 Serial to Ethernet Device Selection

Xtralis recommend using MOXA NPort Servers, specifically the models listed in Table C-1.

Configurations described in this article are based on the functions and features of the Moxa NPort 5110 Serial to Ethernet device.

Note: Refer to product manuals and troubleshooting guides and the MOXA website, located at http://www.moxa.com, for further information.

Model	Ports	Firmware	PC Software	Cable
NPort 5110	1	1.1	NPort Administrator 1.5.9	DB9 – standard extension cable (straight through DB9 male to DB9 female)
NPort 5610-16	16	2.1	NPort Administrator 1.5.9	RJ45 – Moxa part # CBL-RJ45M9-150
NPort 5410	4	2.2	NPort Administrator 1.5.9	DB9 – standard extension cable (straight through DB9 male to DB9 female)
NPort 5210	2	2.0	NPort Administrator 1.5.9	RJ45 – Moxa part # CBL-RJ45M9-150

Table C-1: MOXA NPort Serial to Ethernet Devices

To assemble an RS232 to RJ45 cable, refer to the pinout table below (Table C-2).

DB9 Male Pin	RJ45 Pin
1	6
2	5
3	4
4	8
5	3
6	1
7	2
8	7
9	NC

Table C-2: Pinouts for an RS232 to RJ45 cable

C.3 Network Requirements

For each Serial to Ethernet Device:

- **1 static IP Address -** This address must not end in .255 (e.g. 192.168.1.255), and should be accessible from the Monitoring Computer.
- **1 network port -** This port should be unrestricted, or have restrictions relaxed for communications between the Monitoring Computer and the Serial to Ethernet device. Where port restrictions are in place, the following ports should be unblocked:
  - TCP ports 950-981, 4000 and 4900
  - UDP ports 1029 and 4800

C.4 Software Installation and Configuration

Prerequisites

- Approximately 2.5MB of disk space.
- A ZIP file management program, for example Winzip, WinRAR or 7-Zip.
- Uninstall any installations of NPort Administrator.
- Obtain the latest copy of the NPort Administrator application from http://www.moxa.com.

Installation

1. Open the NPort Administrator zip file and run the installer program.
2. Follow the prompts to install the NPort Administrator.

C.4.1 IP Address and Operating Mode Configuration

1. Open NPort Administrator software.
2. Click on **Search** from the toolbar.
   The software will search for all Moxa devices on the network. The model number, MAC Address and IP address of each Moxa will be displayed under Configuration.

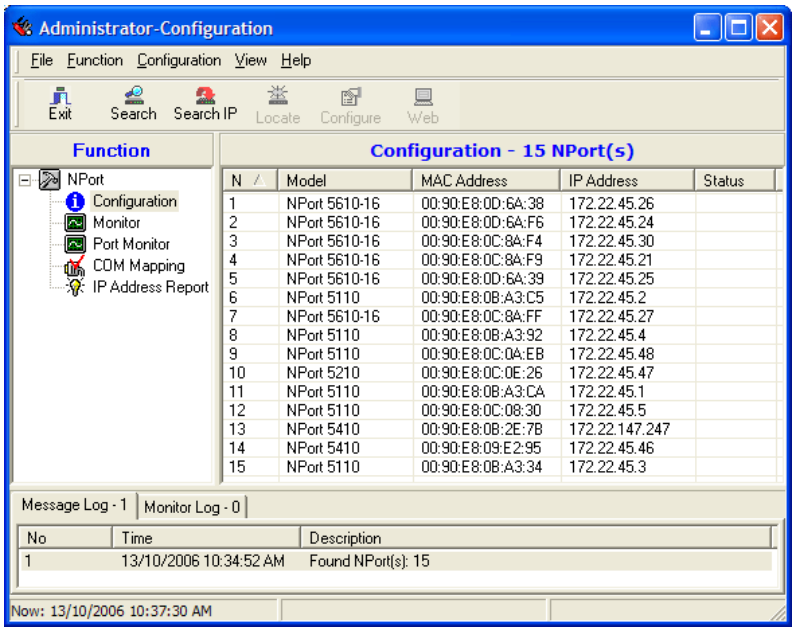

Administrator-Configuration
File Function Configuration View Help
Exit Search Search IP Locate Configure Web
Function
Configuration - 15 NPort(s)
NPort
Configuration
Monitor
Port Monitor
COM Mapping
IP Address Report
N Model MAC Address IP Address Status
1 NPort 5610-16 00:90:E8:0D:6A:38 172.22.45.26
2 NPort 5610-16 00:90:E8:0D:6A:F6 172.22.45.24
3 NPort 5610-16 00:90:E8:0C:8A:F4 172.22.45.30
4 NPort 5610-16 00:90:E8:0C:8A:F9 172.22.45.21
5 NPort 5610-16 00:90:E8:0D:6A:39 172.22.45.25
6 NPort 5110 00:90:E8:0B:A3:C5 172.22.45.2
7 NPort 5610-16 00:90:E8:0C:8A:FF 172.22.45.27
8 NPort 5110 00:90:E8:0B:A3:92 172.22.45.4
9 NPort 5110 00:90:E8:0C:0A:EB 172.22.45.48
10 NPort 5210 00:90:E8:0C:0E:26 172.22.45.47
11 NPort 5110 00:90:E8:0B:A3:CA 172.22.45.1
12 NPort 5110 00:90:E8:0C:08:30 172.22.45.5
13 NPort 5410 00:90:E8:0B:2E:7B 172.22.147.247
14 NPort 5410 00:90:E8:09:E2:95 172.22.45.46
15 NPort 5110 00:90:E8:0B:A3:34 172.22.45.3
Message Log - 1
Monitor Log - 0
No Time Description
1 13/10/2006 10:34:52 AM Found NPort(s): 15
Now: 13/10/2006 10:37:30 AM

Figure C-2: NPort Administrator - Search Results

3. Select the NPort model and then from the toolbar click on Configure. The Configuration screen will be displayed in a separate window.

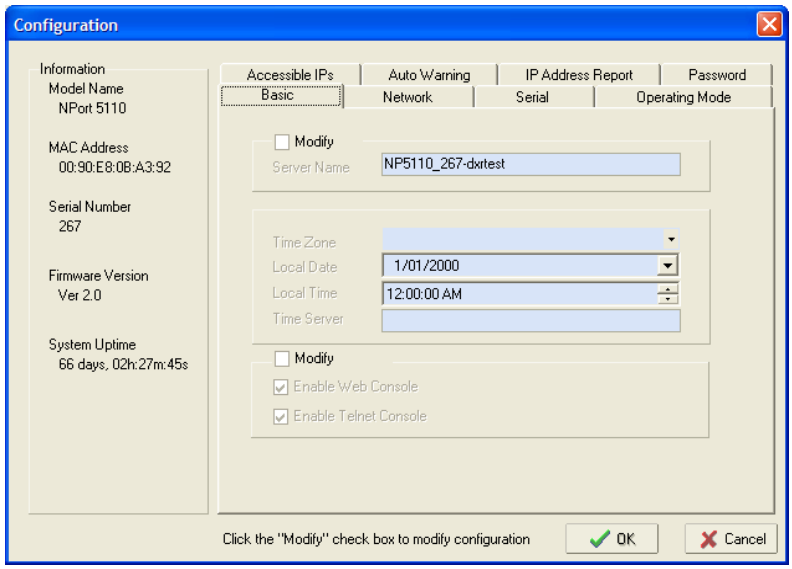


Figure C-3: NPort Administrator - Basic Configuration

4. Select the **Network** tab and then check the **Modify** box.
   Enter the IP address provided by your IT department in the text box provided. Do not use the default IP address.

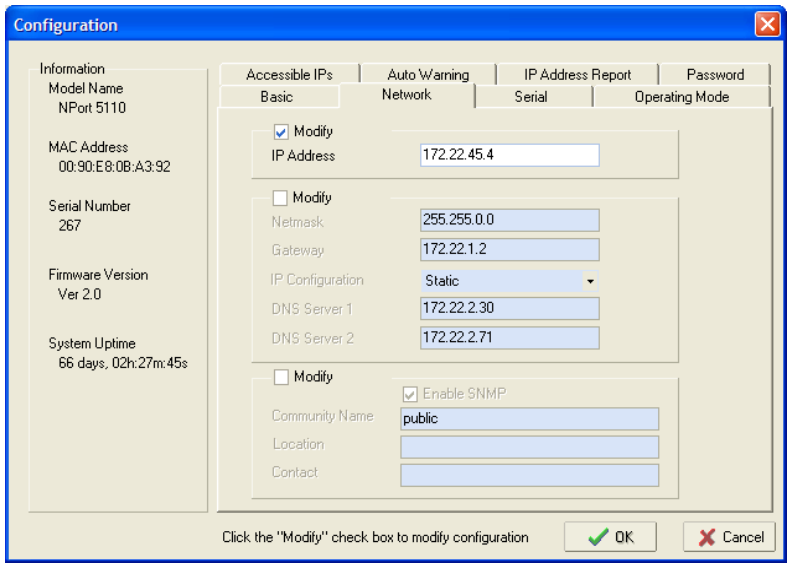


Figure C-4: NPort Administrator - Network Configuration

5. Select the **Operating Mode** tab.
   The Operating Mode should default to Real COM Mode. If it is set differently to Real COM Mode, select the Modify box then click on the Port and then on Settings. Select Real COM Mode from the drop down menu, then select **OK**.

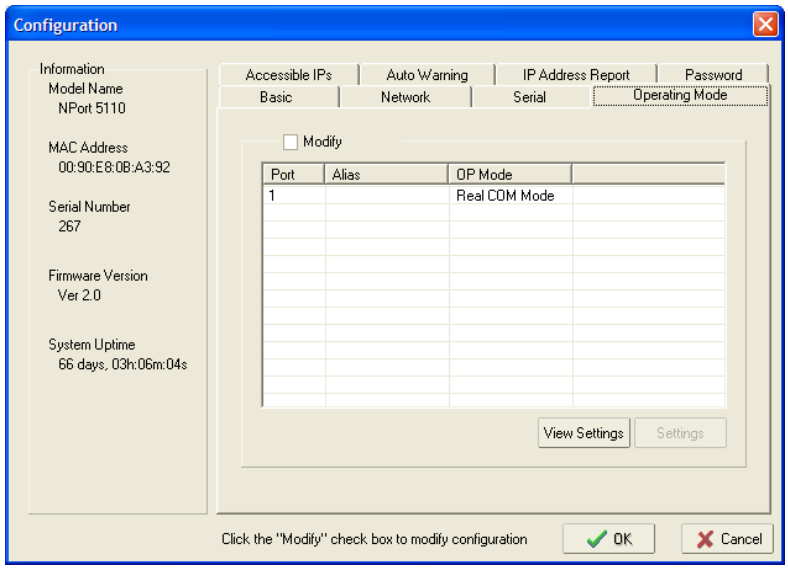


Figure C-5: NPort Administrator - Operating Mode Configuration

6. Click on **OK** from the Configuration screen.
   A dialogue box will confirm that the changes have been applied. Do not change any of the other settings within the remaining configuration tabs.

C.4.2 COM Port Mapping

1. Select COM Mapping, located under the NPort tree.

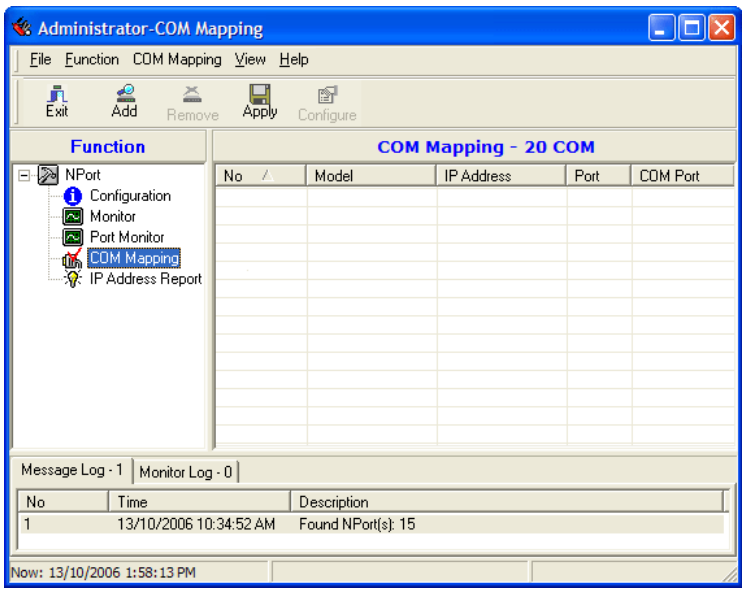


Figure C-6: NPort Administrator - Select COM Mapping

2. From the toolbar, select **Add**.
   A list of all NPort devices will be displayed in a separate window.
3. By default, all NPort devices are checked. Select **Clear All** and then check the box next to the desired NPort device.
   Select an NPort device from the list provided, then select **OK**.
   Do not input the IP address manually.

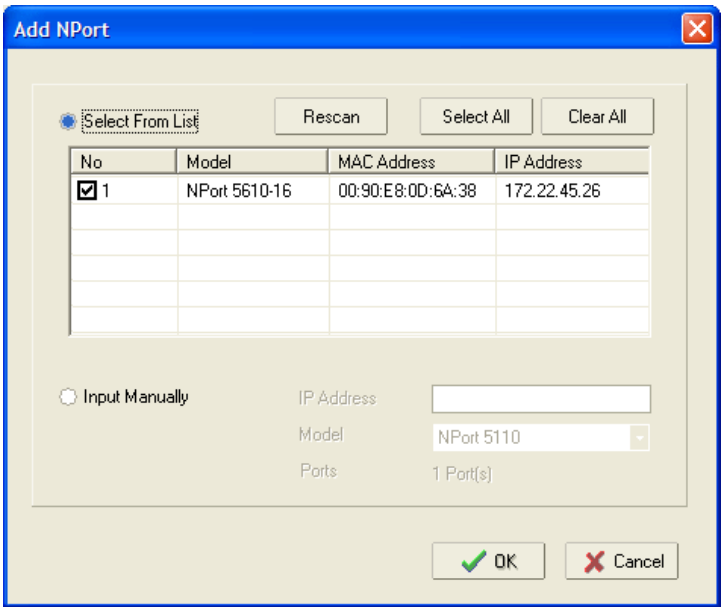


Figure C-7: NPort Administrator - Add NPort

Note: If OK is selected before Clear All, all NPort devices will be displayed under COM Mapping - 1 COM. Select **COM Mapping > Discard Changes** to undo.

4. The NPort device will be displayed on the COM Mapping list.

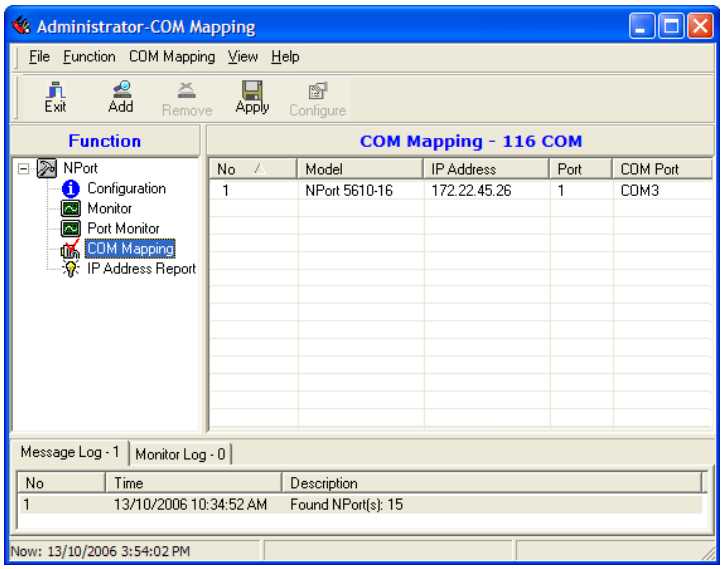


Figure C-8: NPort Administrator - New Port

5. Select NPort device from the COM Mapping list, then select Configure, located on the toolbar. The COM Port Settings configuration window will be displayed.
   - A COM Port is automatically selected and shown in the field labeled COM Number under the Basic Settings tab.
   - The software automatically assigns the next available COM Port. If an alternate COM port number is needed, select it from the drop down menu.
   - The COM Port automatically selected should be added to the list of COM Ports. Confirm that the new COM Port did not override any existing COM Ports.
   - Do not change any of the settings in the Advanced Settings or Serial Parameters tabs. VSM4 automatically configures this information.

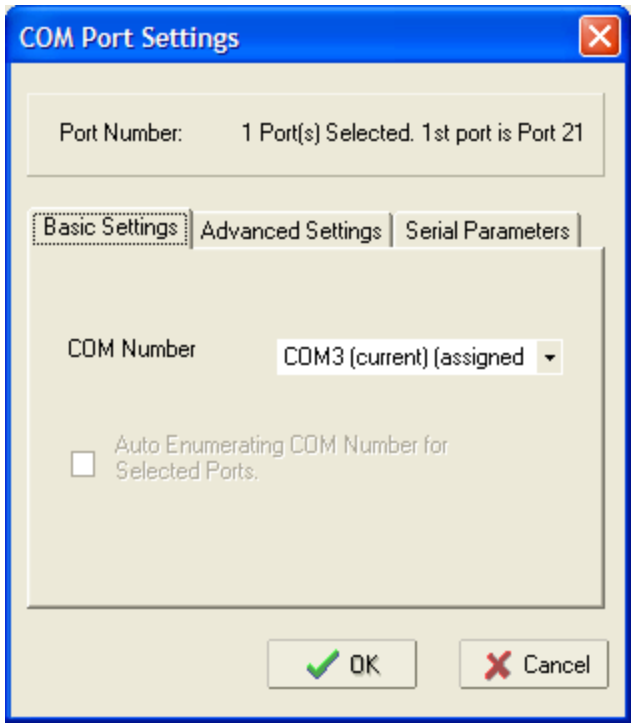


Figure C-9: NPort Administrator - COM Port Settings

6. Select **OK** to set the COM Port and return to the main screen.
7. Select **Apply** from the toolbar to save configuration changes, and **Yes** to confirm.
8. A prompt offers to change the firmware operating mode to Real COM. The firmware operating mode was set to Real COM while setting IP Address for the NPort device. Select **OK** to complete the COM Port Mapping.

C.4.3 Create and test a new Connection

1. Create a new connection to the device on the newly mapped COM Port, as described in Appendix D.
2. Connect to the device, as described in Appendix D.

D Define a Connection

In order to be able to define a connection to a network or standalone detector, follow this procedure:

1. Select **Connection > Manager** from the menu system.
   The Connection Manager dialog is displayed.

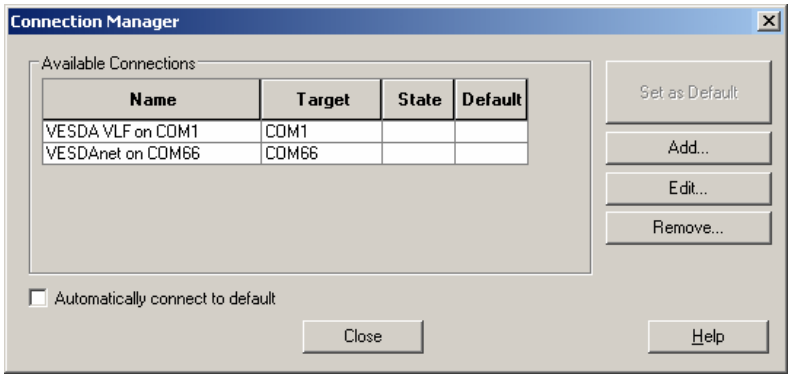


Figure D-1: Connection Manager

Note: If you already have the Open Connection dialog open, access the Connection Manager by selecting Details.

2. Select **Add**.
   The Add Connection dialog is displayed.

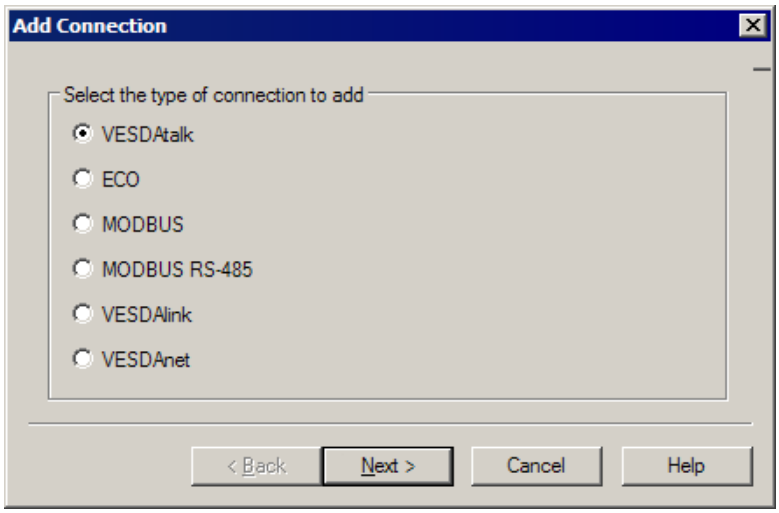


Figure D-2: Add Connection

D.1 VESDAnet Connection via HLI

a. Select **VESDAnet** and click **Next**.
The Select Port dialog appears.

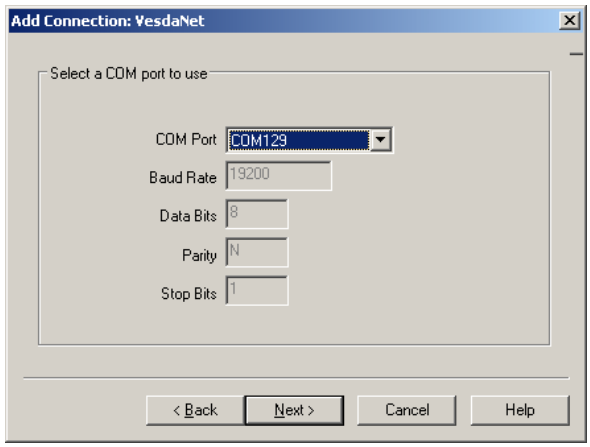


Figure D-3: Select COM Port

b. Select the COM Port associated with the HLI.
Refer to Appendix C for information regarding the mapping of Serial to Ethernet devices to COM Ports.

c. Select **Next**.
The Save Connection dialog appears.

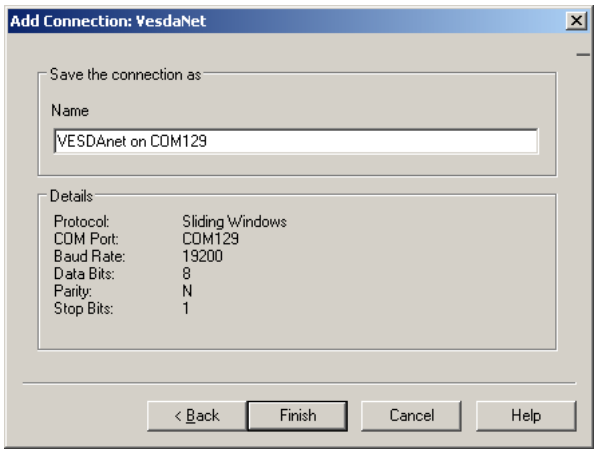


Figure D-4: Save Connection

d. Enter a name for the connection.
e. Select **Finish**.

The connection is added to the list of available connections in the Connection Manager dialog.

D.2 MODBUS RS-485 Connection via RS232-RS485 Converter

a. Select **MODBUS RS-485** and click **Next**.
The Select Port dialog appears.

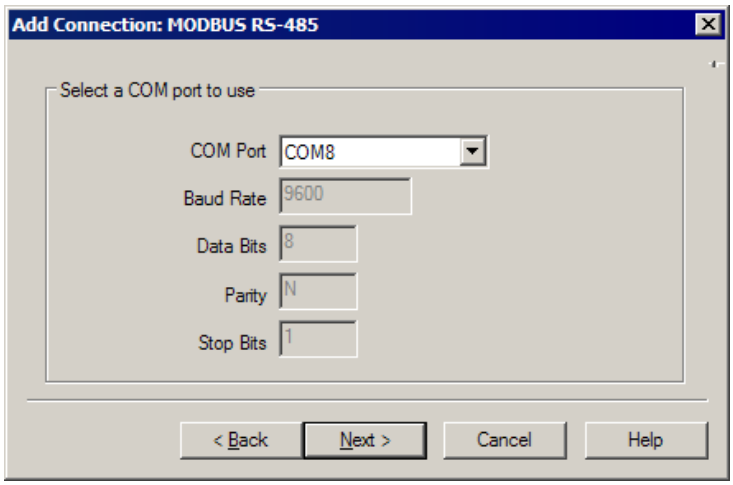


Figure D-5: Select COM Port

b. Select the COM Port associated with the RS232-RS485 converter.
c. Select **Next**.
The Save Connection dialog appears.

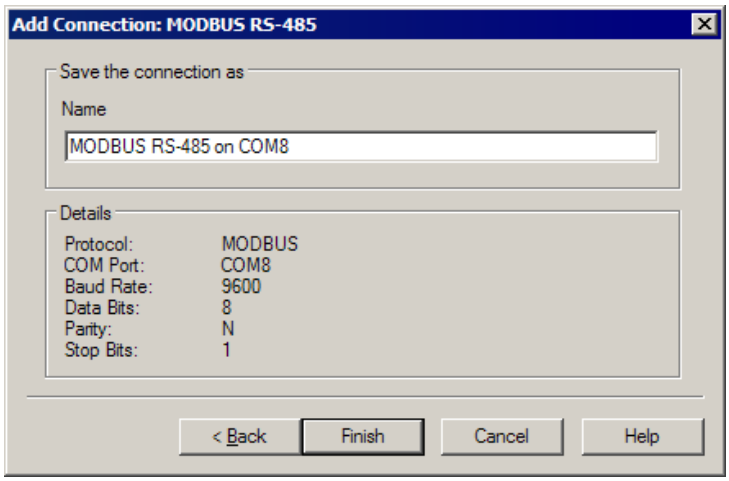


Figure D-6: Save Connection

d. Enter a name for the connection.
e. Select **Finish**.

The connection is added to the list of available connections in the Connection Manager dialog.

D.3 VESDAtalk and VESDAlink Standalone Device Connection

a. To connect to VLF detectors, select **VESDAtalk**, or to connect to VLC-RO detectors, select **VESDAlink**, and click **Next**.
The Select Port screen appears.

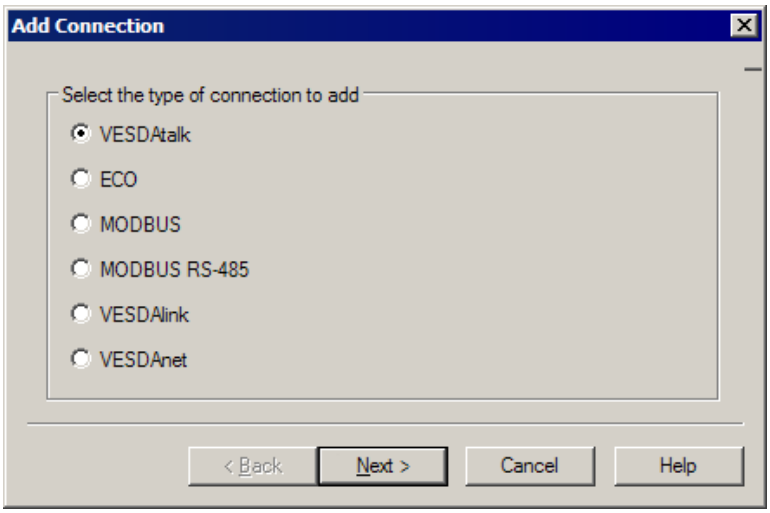


Figure D-7: Add Connection

b. Select the COM port that the detector is connected to and click **Next**.

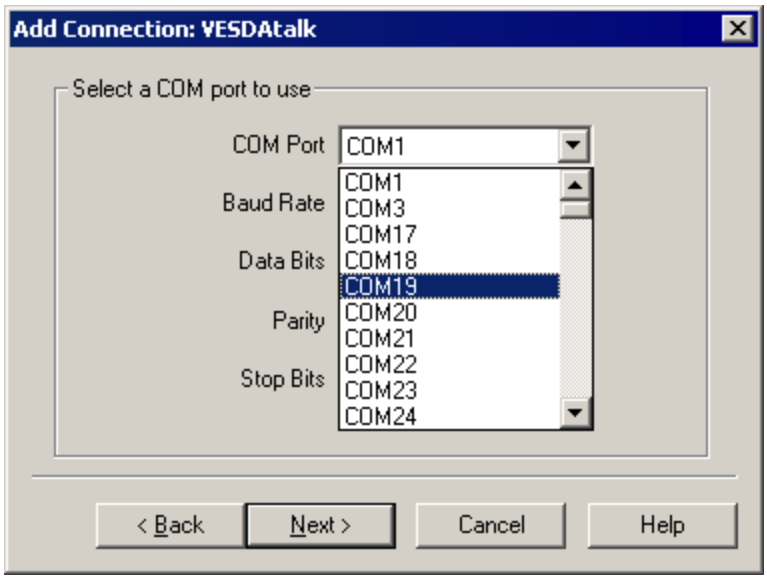


Figure D-8: Select COM Port

c. In the **Name** field, enter a name for the connection. This will be used to refer to this connection. Click **Finish**.

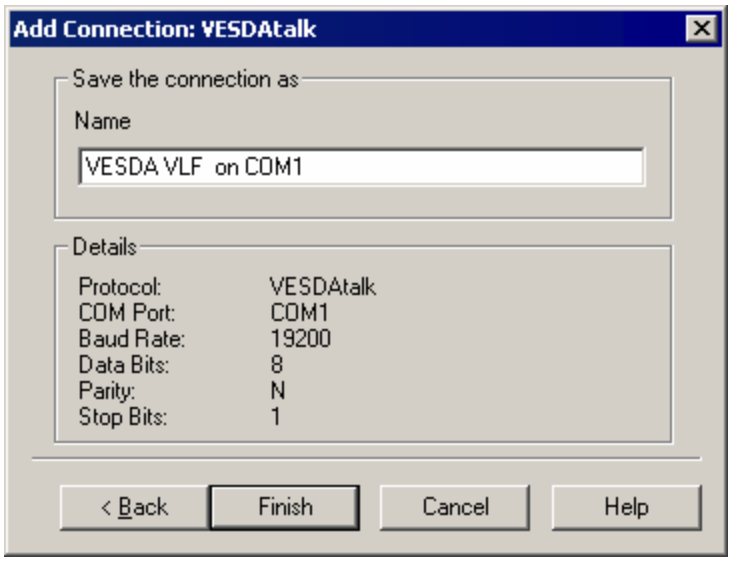


Figure D-9: Connection Name

The connection is added to the list of available connections in the Connection Manager dialog.

d. Ensure that Flow Control is set to None for the COM Port in use.
   - For local COM Ports, this is done in Windows Device Manager.
   - For Virtual COM Ports, this is done in NPort Administrator.

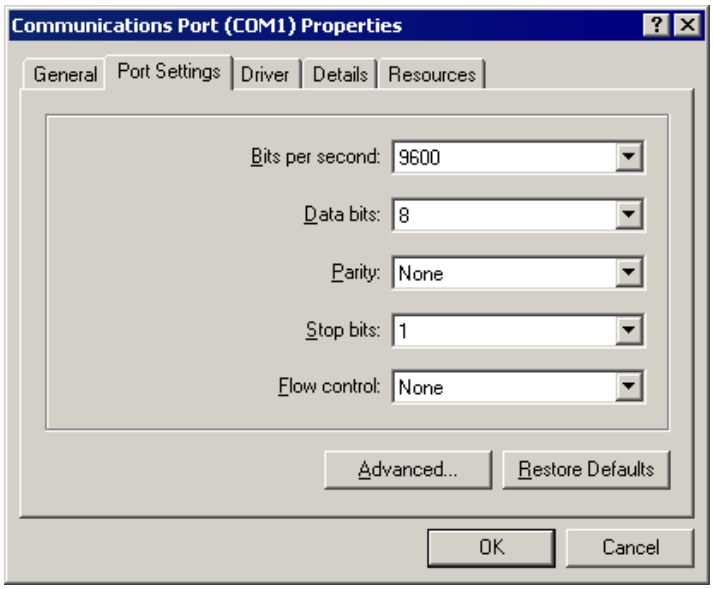


Figure D-10: COM Port Configuration

D.4 RS-232 MODBUS Standalone Device Connection

a. To connect to an IFT or VFT detector using Modbus over an RS-232 direct serial connection, select **MODBUS**, and click **Next**.

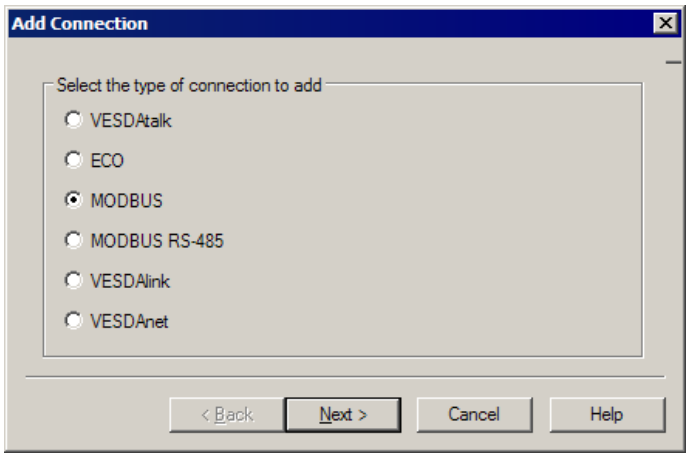


Figure D-11: Add Connection

b. Select **Direct Serial Cable** and click **Next**.

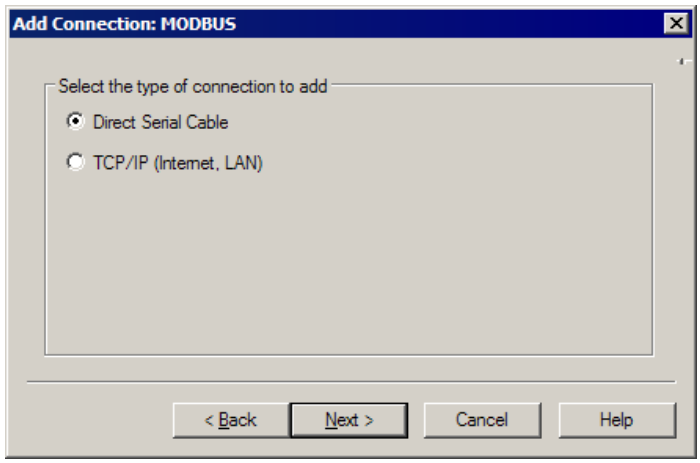


Figure D-12: Select Direct Serial Cable connection

c. Select the COM port that the detector is connected to and click **Next**.

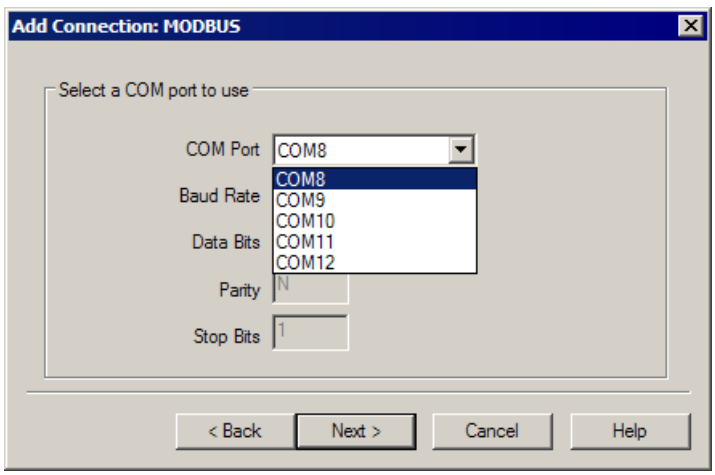


Figure D-13: Select COM Port

d. In the **Name** field, enter a name for the connection. This will be used to refer to this connection. Click **Finish**.

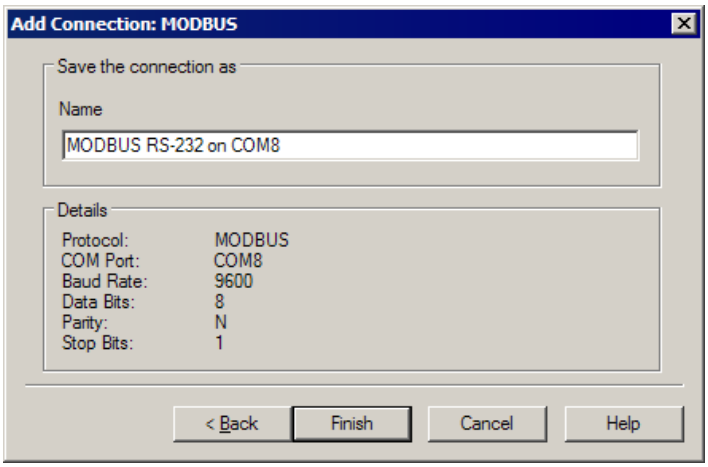


Figure D-14: Connection Name

The connection is added to the list of available connections in the Connection Manager dialog.

e. Ensure that Flow Control is set to None for the COM Port in use.
   - For local COM Ports, this is done in Windows Device Manager.
   - For Virtual COM Ports, this is done in NPort Administrator.

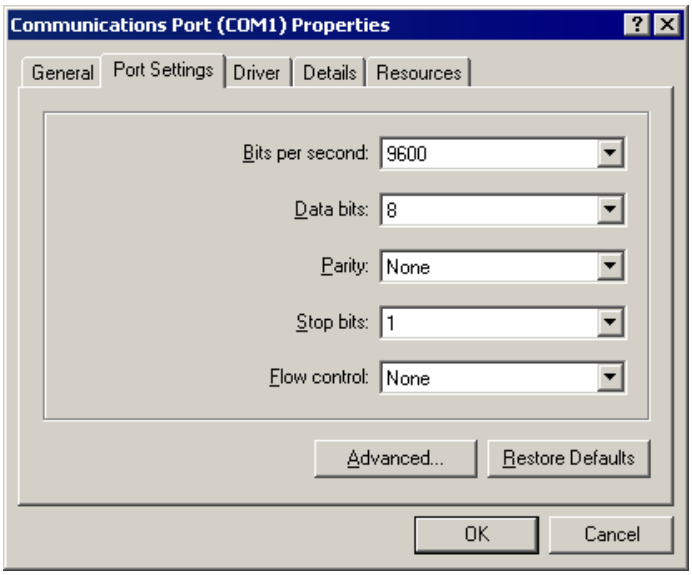


Figure D-15: COM Port Configuration

D.5 TCP/IP MODBUS Standalone Device Connection

a. For connecting to individual IFT or VFT detectors with MODBUS over TCP/IP connection, select **MODBUS** and click **Next**.
The Select Port screen appears.

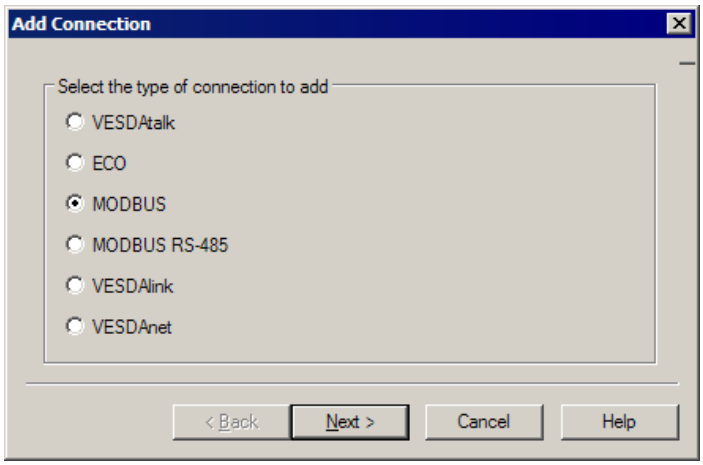


Figure D-16: Add Connection

b. Select **TCP/IP (Internet, LAN)** and click **Next**.

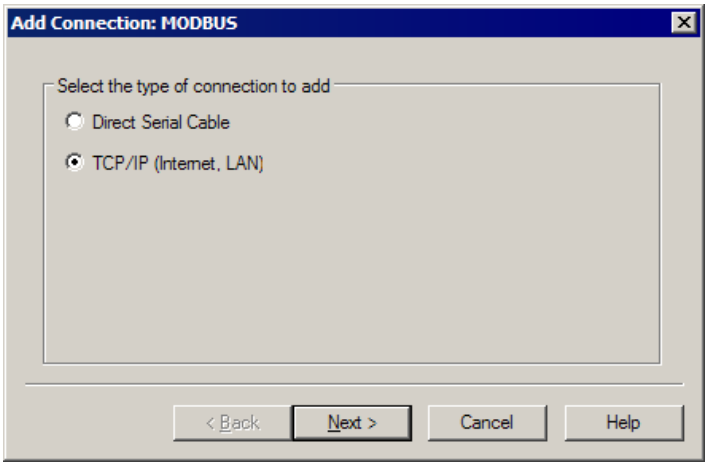


Figure D-17: Select TCP/IP connection

c. Enter the IP address of the remote device and click **Next**.

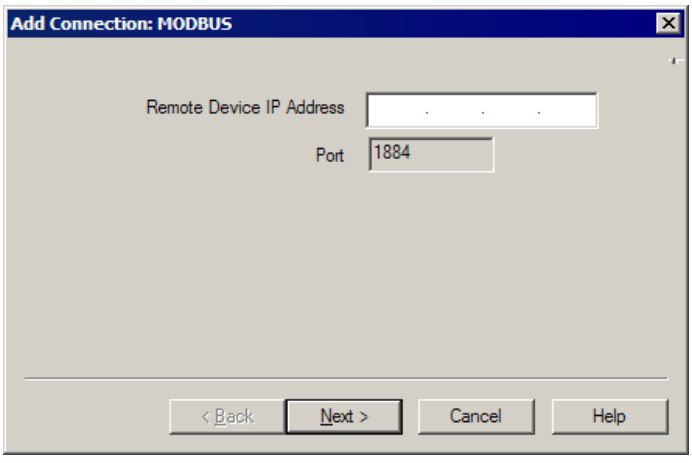


Figure D-18: Enter IP Address

d. In the **Name** field, enter a name for the connection. This will be used to refer to this connection. Click **Finish**.

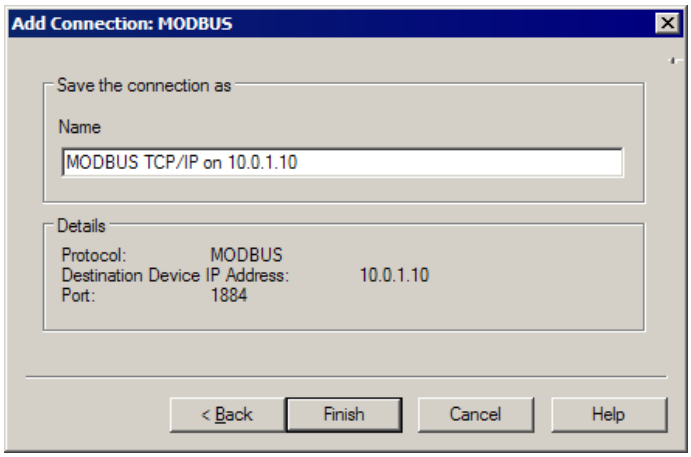


Figure D-19: Connection Name

The connection is added to the list of available connections in the Connection Manager dialog.

This page is intentionally left blank.